

00862.023495



IFW

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)	
	:	Examiner: Unassigned
Junichi HAYASHI)	
	:	Group Art Unit: Unassigned
Application No.: 10/789,986)	
	:	
Filed: March 2, 2004)	
	:	
For: IMAGE DATA ENCRYPTION)	June 21, 2004
METHOD, IMAGE DATA	:	
TRANSFORM METHOD,)	
APPARATUS FOR THE	:	
METHODS, COMPUTER)	
PROGRAM, AND COMPUTER-	:	
READABLE STORAGE MEDIUM)	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBMISSION OF PRIORITY DOCUMENT

Sir:

In support of Applicant's claim for priority under 35 U.S.C. § 119, enclosed is a certified copy of the following Japanese application:

JP 2003-061863, filed March 7, 2003.

Applicants' undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our address given below.

Respectfully submitted,

Attorney for Applicants
Brian L. Klock
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

BLK/lmj

101789, 98e

Juruchi HAYASHI

Image Data Encryption Method, Image Data Transform Method,
Apparatus For the Methods, Computer Program, And Computer-
Readable Storage medium

CFM03495

US

日本国特許庁

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月 7日
Date of Application:

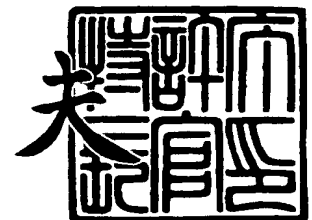
出願番号 特願2003-061863
Application Number:
[ST. 10/C]: [JP 2003-061863]

出願人 キヤノン株式会社
Applicant(s):

2004年 3月22日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2004-3023125

【書類名】 特許願

【整理番号】 253503

【提出日】 平成15年 3月 7日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/00

【発明の名称】 画像データの暗号化方法及び画像データ変換方法、及び、それらの装置、並びにコンピュータプログラム及びコンピュータ可読記憶媒体

【請求項の数】 26

【発明者】

 【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

 【氏名】 林 淳一

【特許出願人】

 【識別番号】 000001007

 【氏名又は名称】 キヤノン株式会社

【代理人】

 【識別番号】 100076428

 【弁理士】

 【氏名又は名称】 大塚 康德

【選任した代理人】

 【識別番号】 100112508

 【弁理士】

 【氏名又は名称】 高柳 司郎

【選任した代理人】

 【識別番号】 100115071

 【弁理士】

 【氏名又は名称】 大塚 康弘

【選任した代理人】

【識別番号】 100116894

【弁理士】

【氏名又は名称】 木村 秀二

【手数料の表示】

【予納台帳番号】 003458

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0102485

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像データの暗号化方法及び画像データ変換方法、及び、それらの装置、並びにコンピュータプログラム及びコンピュータ可読記憶媒体

【特許請求の範囲】

【請求項 1】 画像データを暗号化する画像データ暗号化方法であって、複数のデータブロックで構成される画像データを、前記データブロック単位に

入力したデータブロックが暗号化対象であるか否かを判定する判定工程と、
該判定工程で暗号化対象のデータブロックが入力された場合、当該データブロックを暗号化する暗号化工程と、

復号する際の有意なデータの終端位置を特定するための終端情報を、前記暗号化工程で暗号化されたデータブロックの先頭位置に付加する付加工程と、

前記付加工程を実行するか否かを切り換える切り換え工程と、

前記判定工程で暗号化対象外と判定されたデータブロック、前記切り換え工程のもとで生成されたデータブロックを出力する出力工程と

を備えることを特徴とする画像データの暗号化方法。

【請求項 2】 更に、

前記終端情報を、データブロックの後端位置に付加する第 2 の付加工程とを備え、

前記切り換え工程は、前記付加工程、前記第 2 の付加工程とを切り換えることを特徴とする請求項 1 に記載に記載の画像データの暗号化方法。

【請求項 3】 暗号化されているか否かを示す情報を、前記終端情報の直後に付加することを特徴とする請求項 2 に記載の画像データの暗号化方法。

【請求項 4】 前記終端情報を付加する工程は、暗号化された画像データと置換することを特徴とする請求項 1 乃至 3 のいずれか 1 項に記載の画像データの暗号化方法。

【請求項 5】 前記判定工程の判定は、入力したデータブロックが、予め暗号化対象として設定された対象であるか否かを判定することで行ない、

前記切り換え工程は、暗号化されたデータブロックを、非暗号化のデータブロ

ックと同じ扱いで復号処理に渡して良いか否かの設定情報に従って切り換えることを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の画像データの暗号化方法。

【請求項 6】 更に、画像データを圧縮符号化する符号化工程を備え、前記入力工程は圧縮符号化後の画像データを入力することを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の画像データの暗号化方法。

【請求項 7】 前記符号化工程は、空間領域のデータを周波数領域のデータに変換する周波数変換工程と、

前記周波数領域のデータを量子化し量子化インデックスを算出する量子化工程と、

前記量子化インデックスをエントロピ符号化するエントロピ符号化工程とを有することを特徴とする請求項 6 に記載の画像データの暗号化方法。

【請求項 8】 前記エントロピ符号化工程は、

所定の周波数領域を少なくとも一つ以上の互いに重ならない複数の矩形領域に分割する領域分割工程と、

前記矩形領域毎にビットプレーン単位で、前記量子化インデックスをエントロピ符号化するエントロピ符号化工程と、

前記矩形領域内のエントロピ符号列を少なくとも一つ以上の符号列の集合に分割するエントロピ符号列分割工程と

とを特徴とする請求項 7 に記載の画像データの暗号化方法。

【請求項 9】 前記付加工程は、前記矩形領域内の符号列の集合毎に、前記終端情報を付与することを特徴とする請求項 8 に記載の画像データの暗号化方法。

【請求項 10】 前記符号化工程は、

空間領域のデータを周波数領域のデータに変換する周波数変換工程と、

前記周波数領域のデータを量子化し量子化インデックスを算出する量子化工程と、

前記量子化インデックスをエントロピ符号化するエントロピ符号化工程とを有

し、

前記暗号化工程は、前記エントロピ符号化されたエントロピ符号列に対して暗号化処理を実行することを特徴とする請求項 6 に記載の画像データの暗号化方法。

【請求項 11】 前記符号化工程は、

空間領域のデータを周波数領域のデータに変換する周波数変換工程と、

前記周波数領域のデータを量子化し量子化インデックスを算出する量子化工程と、

前記量子化インデックスをエントロピ符号化するエントロピ符号化工程とを有し、

前記暗号化工程は、前記量子化された量子化インデックスに対して暗号化処理を実行することを特徴とする請求項 6 に記載の画像データの暗号化方法。

【請求項 12】 前記符号化工程は、

空間領域のデータを周波数領域のデータに変換する周波数変換工程と、

前記周波数領域のデータを量子化し量子化インデックスを算出する量子化工程と、

前記量子化インデックスをエントロピ符号化するエントロピ符号化工程とを有し、

前記暗号化工程は、前記周波数変換された周波数領域のデータに対して暗号化処理を実行することを特徴とする請求項 6 に記載の画像データの暗号化方法。

【請求項 13】 前記エントロピ符号化工程は、

所定の周波数領域を少なくとも一つ以上の互いに重ならない複数の矩形領域に分割する領域分割工程と、

前記矩形領域毎にビットプレーン単位でエントロピ符号化しエントロピ符号列を生成するエントロピ符号化工程と、

前記矩形領域内のエントロピ符号列を少なくとも一つ以上の符号列の集合に分割するエントロピ符号列分割工程と

を備えることを特徴とする請求項 10 乃至 12 のいずれか 1 項に記載の画像データの暗号化方法。

【請求項 14】 前記付加工程は、前記矩形領域内の符号列の集合毎に、前記終端情報を付与することを特徴とする請求項 13 に記載の画像データの暗号化方法。

【請求項 15】 暗号化されたデータを含む画像データを再生処理用に変換する画像データ変換方法であって、

複数のデータブロックで構成される画像データを、前記データブロック単位に入力する工程と、

入力したデータブロックが暗号化されているか否かを判定する第 1 の判定工程と、

該判定工程で、暗号化されたデータブロックであると判定した場合、暗号化を解除する鍵情報があるか否かを判定する第 2 の判定工程と、

該第 2 の判定工程で、前記鍵情報があると判定した場合、入力したデータブロックの暗号化を前記鍵情報に従って復号すると共に、当該暗号復号するデータブロックの先頭位置に有意なデータの終端位置を特定するための終端情報がある場合には前記終端情報を無効化する暗号復号工程と、

該暗号復号工程で暗号復号されたデータブロック、及び、前記第 1 の判定工程で非暗号化であると判定されたデータブロック、及び、前記第 2 の判定工程で前記鍵情報がないと判定されたデータブロックを出力する出力工程と

を備えることを特徴とする画像データ変換方法。

【請求項 16】 前記暗号復号工程での、前記終端情報の無効化は、当該終端情報を削除又は暗号復号したデータブロックの後端に配置することを特徴とする請求項 15 に記載の画像データ変換方法。

【請求項 17】 暗号化されたデータを含む画像データを再生処理用に変換する画像データ変換方法であって、

複数のデータブロックで構成される画像データを、前記データブロック単位に入力する工程と、

入力したデータブロックが暗号化されているか否かを判定する第 1 の判定工程と、

該判定工程で、暗号化されたデータブロックであると判定した場合、暗号化を

解除する鍵情報があるか否かを判定する第2の判定工程と、

該第2の判定工程で、前記鍵情報がないと判定した場合、入力したデータブロックの先頭位置に、有意なデータの終端位置を特定するための終端情報がある場合に、その終端情報を無効化するか否かを判定する第3の判定工程と、

該第3の判定工程で、前記終端情報を無効化すると判定した場合、前記終端情報を除去、もしくはデータブロックの後端に位置させる終端情報無効化工程と、

前記第2の判定工程で前記鍵情報があると判定した場合、入力したデータブロックの暗号化を復号する復号工程と、

前記第1の判定工程で暗号化されていないと判定されたデータブロック、前記第3の判定工程で、前記終端情報を無効化しないと判定されたデータブロック、前記終端情報無効化工程で終端情報が無効化されたデータブロック、及び、前記復号工程で復号されたデータブロックを出力する出力工程と

を備えることを特徴とする画像データ変換方法。

【請求項18】 前記入力工程で入力する画像データは、圧縮符号化されていることを特徴とする請求項15乃至17のいずれか1項に記載の画像データ変換方法。

【請求項19】 更に、前記出力工程で出力された圧縮符号化されたデータブロックを復号する復号工程を備えることを特徴とする請求項18に記載の画像データ変換方法。

【請求項20】 画像データを暗号化する画像データ暗号化装置であって、複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力手段と、

入力したデータブロックが暗号化対象であるか否かを判定する判定手段と、

該判定手段で暗号化対象のデータブロックが入力された場合、当該データブロックを暗号化する暗号化手段と、

復号する際の有意なデータの終端位置を特定するための終端情報を、前記暗号化手段で暗号化されたデータブロックの先頭位置に付加する付加手段と、

前記付加手段を実行するか否かを切り換える切り換え手段と、

前記判定手段で暗号化対象外と判定されたデータブロック、前記切り換え手段

のもとで生成されたデータブロックを出力する出力手段と

を備えることを特徴とする画像データの暗号化装置。

【請求項 21】 暗号化されたデータを含む画像データを再生処理用に変換する画像データ変換装置であって、

複数のデータブロックで構成される画像データを、前記データブロック単位に
入力する入力手段と、

入力したデータブロックが暗号化されているか否かを判定する第 1 の判定手段
と、

該判定手段で、暗号化されたデータブロックであると判定した場合、暗号化を
解除する鍵情報があるか否かを判定する第 2 の判定手段と、

該第 2 の判定手段で、前記鍵情報があると判定した場合、入力したデータブ
ロックの暗号化を前記鍵情報に従って復号すると共に、当該暗号復号するデータ
ブロックの先頭位置に有意なデータの終端位置を特定するための終端情報がある場
合には前記終端情報を無効化する暗号復号手段と、

該暗号復号手段で暗号復号されたデータブロック、及び、前記第 1 の判定手段
で非暗号化であると判定されたデータブロック、及び、前記第 2 の判定手段で前
記鍵情報がないと判定されたデータブロックを出力する出力手段と

を備えることを特徴とする画像データ変換装置。

【請求項 22】 暗号化されたデータを含む画像データを再生処理用に変換
する画像データ変換装置であって、

複数のデータブロックで構成される画像データを、前記データブロック単位に
入力する入力手段と、

入力したデータブロックが暗号化されているか否かを判定する第 1 の判定手段
と、

該判定手段で、暗号化されたデータブロックであると判定した場合、暗号化を
解除する鍵情報があるか否かを判定する第 2 の判定手段と、

該第 2 の判定手段で、前記鍵情報がないと判定した場合、入力したデータブ
ロックの先頭位置に、有意なデータの終端位置を特定するための終端情報がある場
合に、その終端情報を無効化するか否かを判定する第 3 の判定手段と、

該第3の判定手段で、前記終端情報を無効化すると判定した場合、前記終端情報を除去、もしくはデータブロックの後端に位置させる終端情報無効化手段と、

前記第2の判定手段で前記鍵情報があると判定した場合、入力したデータブロックの暗号化を復号する復号手段と、

前記第1の判定手段で暗号化されていないと判定されたデータブロック、前記第3の判定手段で、前記終端情報を無効化しないと判定されたデータブロック、前記終端情報無効化手段で終端情報が無効化されたデータブロック、及び、前記復号手段で復号されたデータブロックを出力する出力手段と

を備えることを特徴とする画像データ変換装置。

【請求項23】 画像データを暗号化する画像データ暗号化装置として機能するコンピュータプログラムであって、

複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力手段と、

入力したデータブロックが暗号化対象であるか否かを判定する判定手段と、

該判定手段で暗号化対象のデータブロックが入力された場合、当該データブロックを暗号化する暗号化手段と、

復号する際の有意なデータの終端位置を特定するための終端情報を、前記暗号化手段で暗号化されたデータブロックの先頭位置に付加する付加手段と、

前記付加手段を実行するか否かを切り換える切り換え手段と、

前記判定手段で暗号化対象外と判定されたデータブロック、前記切り換え手段のもとで生成されたデータブロックを出力する出力手段と

して機能することを特徴とするコンピュータプログラム。

【請求項24】 暗号化されたデータを含む画像データを再生処理用に変換する画像データ変換装置として機能するコンピュータプログラムであって、

複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力手段と、

入力したデータブロックが暗号化されているか否かを判定する第1の判定手段と、

該判定手段で、暗号化されたデータブロックであると判定した場合、暗号化を

解除する鍵情報があるか否かを判定する第2の判定手段と、

該第2の判定手段で、前記鍵情報があると判定した場合、入力したデータブロックの暗号化を前記鍵情報に従って復号すると共に、当該暗号復号するデータブロックの先頭位置に有意なデータの終端位置を特定するための終端情報がある場合には前記終端情報を無効化する暗号復号手段と、

該暗号復号手段で暗号復号されたデータブロック、及び、前記第1の判定手段で非暗号化であると判定されたデータブロック、及び、前記第2の判定手段で前記鍵情報がないと判定されたデータブロックを出力する出力手段と

して機能することを特徴とするコンピュータプログラム。

【請求項25】 暗号化されたデータを含む画像データを再生処理用に変換する画像データ変換装置として機能するコンピュータプログラムであって、

複数のデータブロックで構成される画像データを、前記データブロック単位に入力する入力手段と、

入力したデータブロックが暗号化されているか否かを判定する第1の判定手段と、

該判定手段で、暗号化されたデータブロックであると判定した場合、暗号化を解除する鍵情報があるか否かを判定する第2の判定手段と、

該第2の判定手段で、前記鍵情報がないと判定した場合、入力したデータブロックの先頭位置に、有意なデータの終端位置を特定するための終端情報がある場合に、その終端情報を無効化するか否かを判定する第3の判定手段と、

該第3の判定手段で、前記終端情報を無効化すると判定した場合、前記終端情報を除去、もしくはデータブロックの後端に位置させる終端情報無効化手段と、

前記第2の判定手段で前記鍵情報があると判定した場合、入力したデータブロックの暗号化を復号する復号手段と、

前記第1の判定手段で暗号化されていないと判定されたデータブロック、前記第3の判定手段で、前記終端情報を無効化しないと判定されたデータブロック、前記終端情報無効化手段で終端情報が無効化されたデータブロック、及び、前記復号手段で復号されたデータブロックを出力する出力手段と

して機能することを特徴とするコンピュータプログラム。

【請求項 2 6】 請求項 2 3 乃至 2 5 のいずれか 1 項に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は画像データの暗号化及び暗号復号技術に関するものである。

【0 0 0 2】

【従来の技術】

画像データなどのアクセス制御を目的として、画像データの暗号化やスクランブルなどが行なわれてきた。これは、予め画像データを暗号鍵を用いて暗号化し、前記暗号鍵に対応する復号鍵を有する者だけが正しく再生できるようにする技術である。

【0 0 0 3】

一方、画像データは情報量が大きいために、これを効率的に伝送、及び蓄積する際に圧縮符号化を行う場合が多い。圧縮符号化としては、例えば、I S O / I E C J T C 1 / S C 2 9 / W G 1 にて標準化されている J P E G 2 0 0 0 規格と呼ばれる技術などが適応される。前述した画像データの暗号化は J P E G 2 0 0 0 規格のような圧縮符号化された画像データに対して施される場合もある。これにより、画像データを効率的に伝送、及び蓄積すると同時に、画像データに対するアクセスを制御できるという利点がある。

【0 0 0 4】

特に、J P E G 2 0 0 0 規格のような圧縮符号化技術によれば、画像データは、解像度、画質、空間的領域、画素を構成する成分などに応じて階層的に圧縮符号化できる。こうした階層構造を有する画像データに対して、階層構造に応じた暗号化処理を行うことにより、階層構造に応じたアクセス制御を実現することができる。

【0 0 0 5】

例えば、解像度毎にアクセス制御する場合、低解像度成分は暗号化せずに、高解像度成分だけ暗号化するようにすれば、低解像度成分は誰でも再生可能である

が、高解像度成分は許可された利用者（復号鍵の所有者）だけが正しく再生するようにアクセス制御できるようになる。

【0 0 0 6】

【発明が解決しようとする課題】

しかしながら、階層構造を有する画像データに当該階層構造に応じた暗号化処理を施した場合、復号鍵を有していない装置では暗号を復号できず、暗号データのままの状態で圧縮復号されるため、画像はスクランブルされた状態となって再生される。即ち、スクランブルされていない状態で画像を再生することは困難であった（例えば、前述した例のように解像度毎にアクセス制御する場合は、高解像度の画像データを再生せずに、低解像度の画像データだけを再生することが困難であった）。

【0 0 0 7】

本発明はかかる問題点に鑑みなされたものであり、画像再生装置でスクランブルさせて再生させるか、或いは、非スクランブル状態で再生させるかを暗号化する側で設定可能とする技術を提供しようとするものである。

【0 0 0 8】

【課題を解決するための手段】

この課題を解決するため、例えば本発明の画像データ暗号化方法は以下の工程を備える。すなわち、

画像データを暗号化する画像データ暗号化方法であって、

複数のデータブロックで構成される画像データを、前記データブロック単位に
入力する工程と、

入力したデータブロックが暗号化対象であるか否かを判定する判定工程と、

該判定工程で暗号化対象のデータブロックが入力された場合、当該データブロックを暗号化する暗号化工程と、

復号する際の有意なデータの終端位置を特定するための終端情報を、前記暗号化工程で暗号化されたデータブロックの先頭位置に付加する付加工程と、

前記付加工程を実行するか否かを切り換える切り換え工程と、

前記判定工程で暗号化対象外と判定されたデータブロック、前記切り換え工程

のもとで生成されたデータブロックを出力する出力工程とを備える。

【0009】

【発明の実施の形態】

以下、添付図面に従って本発明に係る実施形態を説明する。

【0010】

＜全体構成の説明＞

実施形態におけるシステム概要例を図14に示す。図中、140はインターネットであって、141は例えばデジタルカメラやイメージスキャナ、フィルムスキャナ等で撮像した画像データを圧縮符号化&暗号化処理を行う装置である。142は画像データを受信し、復号する装置、143は復号する際に必要となる暗号化解除鍵を記憶している認証サーバある。装置141乃至143はパーソナルコンピュータ等の汎用装置で構わない。処理の流れを簡単に説明すると、次の通りである。

【0011】

装置141では、所望とする画像データを圧縮符号化及び暗号化処理を行い、インターネット140を介して配布する。配布するのは装置141が直接行ってもよいし、適当なサーバを介して配布しても構わない。ただし、暗号化されている関係で、その解除するために必要な鍵情報を、その画像データを特定する情報（例えばID）と共に認証サーバ143が有するDBに登録しておく。画像復号装置142は所望とする画像を受信し、復号を行ない閲覧するものであるが、暗号化されている画像データを閲覧するには、認証サーバ143にその画像を特定する情報を通知して、暗号化解除鍵情報を要求する。この結果、暗号化解除鍵情報が認証サーバ143より受信するので、それを用いて暗号化を解除し、復号再生する。

【0012】

実施形態では説明を簡単なものとするため、暗号化対象の画像（ファイル）はISO/IEC JTC1/SC29/WG1 10918-1において標準化されている、通称JPEG2000と呼ばれる圧縮符号化方式によって符号化されたデータであるものとして説明するが、JPEG2000に本発明が限定される

ことなく、J P E G など種々の圧縮符号化の方式を適応可能であることは以下の説明から明らかになるであろう。

【0013】

さて、装置 141 での暗号化処理の詳細を説明する前に、実施形態における暗号化処理の操作画面（ウインドウ）について図 20 を用いて説明することとする。

【0014】

図示において、200 がそのウインドウを示し、201 は暗号化対象となるファイル（J P E G 2000 による圧縮符号化されたファイル）を指定する欄であり、不図示のキーボードよりファイルのパス付きで指定しても良いし、その欄 201 の右端に設けられたボタンをクリックすることで、ファイルブラウザを表示し、その中で選択しても構わない。202 は選択されたファイルで示される画像（復号処理を行う）を表示する領域である。

【0015】

一方、ウインドウ 200 の右側には、暗号化後の出力ファイル名を入力する欄 203、及び、暗号化を解除する解除鍵のファイル名 204（解除鍵ファイルは、出力ファイルと同じパスに格納されるものとしているので、ファイル名のみ）を入力する欄が設けられている。

【0016】

入力対象の画像が J P E G 2000 による圧縮符号化されているファイルの場合、そのヘッダ部を解析することで、何回のウェーブレット符号化が行われているかが既に決まっていることになる。205 は、そのファイルのウェーブレット変換回数に基づいて、周波数成分をタイルパートにして示す図である。図示の場合、ウェーブレット変換回数が 2 回であるので、タイルパートは 3 つの解像度レベルグループ、すなわち、L L、{L H 2 + H H 2 + H L 2}、及び、{L H 3 + H H 3 + H L 3} に別れて示されている。207 はマウス（登録商標）等のポインティングデバイスに連動して表示されるカーソルである。ユーザは、所望とするタイルパートの上にカーソル 207 を移動させ、その位置でポインティングデバイスが有するボタンをクリックする操作を行うと、そのタイルパートについ

での暗号化処理の設定ウインドウを表示する。図示の 2 0 8 がその設定ウインドウを示している。図示に示す如く、ユーザは該当するタイルパート毎に、暗号化を行うか否か、及び、終端マーカを前、後のいずれにするかを設定することができる（詳細は後述）。なお、これらの項目は 2 者択一であるのでコンボボックスにしているが、ラジオボタンでも構わない。要するに、表示フォーマットによって本願発明が限定されるものではないことを付言しておく。

【 0 0 1 7 】

なお、J P E G 2 0 0 0 の場合、1 画像が複数のタイルで分割されることも有り得る。従って、複数のタイルが存在する場合には、その数に応じた表示を行うことになる。

【 0 0 1 8 】

2 0 9 は本処理を終了させるためのボタンであり、2 1 0 は設定内容に従って暗号化処理を実行開始を行わせるためのボタンである。

【 0 0 1 9 】

ボタン 2 1 0 がクリックされた場合には、設定内容（暗号化対象のサブバンドに関する情報、及び、その暗号化するサブバンドの符号化データに終端マーカをどの位置に配置するかという情報）が一時的に R A M（上記の如く、装置 1 4 1 はパーソナルコンピュータ等の汎用情報処理装置であるので、作業用 R A M は備えている）に一時的に格納し、指定されたオリジナル画像ファイルを読み込み、設定された内容に従って暗号化し、その結果を欄 2 0 3 に記述されたファイルとして出力することになる。

【 0 0 2 0 】

なお、上記例では、タイルパートが解像度毎のグループに分けている例を説明したが、個々のサブバンド毎、例えば、サブバンド L H 3 のみ暗号化を行うように指定してもよいし、複数のタイルパートに対して設定するようにしてもよい。

【 0 0 2 1 】

また、図 2 0 では、ウェブレット変換する対象は画像全体に対するもの、すなわち、1 タイル = 1 画像であるとしたが、タイル数は上記の如く、複数存在数 r 場合も有り得る。従って、この場合には、設定内容には、タイルを特定する情報

も記憶する必要があるし、タイル単位に暗号化する／しないを設定しても構わない。

【0022】

＜暗号化処理部＞

図1は、実施形態における暗号化処理機能を説明する図である。図14における装置141における処理の一部に対応するものでもあり、図20においてボタン210がクリックされた際の装置の処理機能ブロック図であると言えば分かりやすい。なお、処理対象がJ P E G 2 0 0 0以外のデータ形式の場合には、まず、J P E G 2 0 0 0による圧縮符号化が行われることになるが、その詳細は後述することとし、ここでは既にJ P E G 2 0 0 0により圧縮されたものとして説明する。

【0023】

図1において、11はコードストリーム入力部、12はコードストリーム暗号化部、13はコードストリーム出力部、14は図20の画面で設定した内容を保持する暗号化パラメータ部である。

【0024】

コードストリーム入力部11はユーザが指定した画像ファイルをコードストリームとして入力し、それに含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し、必要な場合は処理の流れを制御し、或いは後続の処理ユニットに対して該当するパラメータを送出するものである。入力されたコードストリームPはコードストリーム暗号化部12に出力される。コードストリーム入力部11には、後述する圧縮符号化処理部から出力されるコードストリームを入力するようにする。

【0025】

コードストリーム暗号化部12はコードストリームPを入力し、コードストリームPの、暗号化パラメータ部14よりの設定パラメータにより指定された部分を暗号化処理し、暗号化されたコードストリームCを出力する。コードストリーム暗号化処理部12で実行されるコードストリーム暗号化処理の詳細は後述する。暗号化されたコードストリームCは、コードストリーム出力部13から外部の

記憶装置（例えばハードディスク等）に、ユーザが指定した暗号化後のファイルとして出力される。

【0026】

コードストリーム出力部 13 は、前段のコードストリーム暗号化処理部 12 で暗号化されたコードストリーム C が入力され、暗号化されたコードストリーム C として出力される。また、暗号化を解除する鍵情報は別途作成され、出力されることになる。

【0027】

次に、コードストリーム暗号化処理部 12 で実行されるコードストリーム暗号化処理について、図 2 を用いて説明する。図 2 は本実施形態におけるコードストリーム暗号化処理を説明するフローチャートである。

【0028】

なお、本実施形態におけるコードストリームとは、先に説明したように、ISO/IEC JTC1/SC29/WG1 10918-1 において標準化されている、通称 JPEG 2000 と呼ばれる圧縮符号化方式によって符号化された符号データ列である。従って、コードストリーム入力部 11 はこの符号化データ列を入力することになる。

【0029】

まず、ステップ S21 では、入力されたコードストリーム P のメインヘッダ及びタイルパートヘッダが解析される。ここで、本実施の形態において適応可能なコードストリーム P の構成を図 3 を用いて説明する。

【0030】

JPEG 2000 の圧縮符号化時において、画像は先ず複数の矩形領域に分割され、矩形領域毎にウェーブレット変換により独立に符号化処理が施される。この矩形領域を「タイル」と呼ぶ。尚、JPEG 2000 において、符号化されたタイルに対応するコードストリームは、少なくとも一つ以上のタイルパートと呼ばれる領域に分割できる。JPEG 2000 においては、タイル毎に独立に符号化処理を行うことも可能である。

【0031】

図3（A）は、画像全体が4つのタイルに分割されて圧縮符号化された場合のコードストリームの例を示す。この場合、図3（A）に示すように、コードストリームPは一つのメインヘッダに続いて、4つのタイルパートから構成されることになる。

【0032】

メインヘッダは、符号化対象となる画像のサイズ（水平及び垂直方向の画素数）、タイルサイズ、各色成分を表すコンポーネント数、各成分の大きさ、ビット精度を表すコンポーネント情報から構成されている。

【0033】

次に、本実施形態におけるタイルパートについて説明する。図3（B）は、一つのタイルパートを構成するコードストリームの構成を示す。図3（B）に示すように、タイルパートは一つのタイルパートヘッダに続いて、少なくとも一つ以上のパケットと呼ばれる単位から構成される。

【0034】

なお、通信分野で使われている伝送単位でも「パケット」という表現が使われているが、実施形態で言うパケットとは、通信レベル（プロトコル層）のパケットではなく、アプリケーションレベルのデータの塊を差すことに注意されたい。

【0035】

タイルパートヘッダは当該タイルパートのビットストリーム長とヘッダ長を含めたタイル長及び当該タイルに対する符号化パラメータから構成される。符号化パラメータには離散ウェーブレット変換のレベル（何回ウェーブレットを行ったか）、フィルタ（タップ数の指定）の種類等が含まれている。

【0036】

次に、本実施形態におけるパケットについて説明する。パケットとは、所定の解像度レベル、所定のレイヤ、所定のプレシント、及び所定のコンポーネントにより特定される符号化単位である。また、パケットは、当該パケットに対応するエントロピ符号から構成されるパケットボディ、及び当該パケットボディに関する符号化パラメータを記録したパケットヘッダから構成される。更に、パケットは、図3（C）に示すように、少なくとも一つ以上のコードブロックと呼ばれ

る単位から構成される。解像度レベル、レイヤ、プレシント、コンポーネント、及びコードブロックについての詳細は後述する。従って、このパケットヘッダを解析すると、当該パケットが如何なる解像度レベル（図20の周波数成分グループに対応する）、レイヤ、プレ辛苦と、及びコンポーネントに属するかが判別可能となっている。より分かりやすく説明するのであれば、注目パケットが暗号化対象か否かが判別できることを意味する。

【0037】

以上、本実施の形態において適応可能なコードストリームPの構成を説明した

。

【0038】

図2に示すフローチャートの説明に戻る。ステップS22では、パラメータjが0に初期化される。jはパケットを特定するパラメータである。続いて、ステップS23では特定されたパケットjが暗号化対象であるか否かを、暗号化パラメータ部14からの情報に従って判定される。パケットjが暗号化対象である場合には処理をステップS24に進め、暗号化対象でない場合には処理をステップS25に進める。

【0039】

暗号化対象か否かの設定は、先に図20で説明した通りであるが、例えば、暗号化パラメータを別途ファイルとして保存しておき、それを使い回しするようにしても構わない。

【0040】

いずれにしても、「低解像度は誰にでも閲覧可能とし、高解像度は許可されたユーザだけ閲覧可能とする」ようなアクセス制御を行う場合には、ステップS23において高解像度レベルに対応するパケットだけを暗号化対象とし、低解像度レベルに対応するパケットは暗号化対象としないように設定することになる。また、「領域Aは誰にでも閲覧可能とし、領域Bは許可されたユーザだけ閲覧可能とする」ようなアクセス制御を行う場合（タイルが複数存在する場合、或いは特定のサブバンドのみを暗号化する場合等）には、その領域Bに対応するパケットだけを暗号化対象とし、領域Aに対応するパケットは暗号化対象としないように

設定すればよい。

【0041】

また、予めコードストリームに含まれる全てのパケットが暗号化対象である場合には、ステップS23における判定処理を省略することも可能である。更に、後述するパケット暗号化処理内において暗号化対象とするコードブロックを判定するような場合にも、ステップS23における判定処理を省略することが可能である。

【0042】

次に、ステップS24では、パケットjに対して、パケット暗号化処理が施される。パケット暗号化処理の詳細は後述する。そして、ステップS25では、パラメータjの値が1だけ増やされ、ステップS26でパラメータjとMの値が比較される。ここでMはコードストリームに含まれるパケットの総数である。jがMより小さいときは処理をステップS23に進め、jがM以上の時にはコードストリーム暗号化処理を終了する。

【0043】

以上、本実施形態におけるコードストリーム暗号化処理について説明した。

【0044】

次に、本実施の形態におけるパケット暗号化処理の詳細について、図4を用いて説明する。すなわち、暗号化対象のパケットであると判断した場合の処理である。

【0045】

まず、ステップS41では、入力されたパケットjのパケットヘッダが解析され、当該パケットに含まれるコードブロック等の構造が解析される。その後、ステップS42ではパラメータiが0に初期化される。iはコードブロックを特定するパラメータである。続いて、ステップS43では、特定されたコードブロックiが暗号化対象であるか否かが判定される。コードブロックiが暗号化対象である場合には処理をステップS44に進め、暗号化対象でない場合には処理をステップS48に進める。

【0046】

尚、前述した図2におけるステップS23などにより、予めパケットに含まれる全てのコードブロックが暗号化対象であることが既知である場合には、ステップS43における判定処理を省略することも可能である。

【0047】

続いて、ステップS44では、コードブロック*i*に暗号化処理が施される。本実施形態においては特に暗号化アルゴリズムについては特に限定しないが、例えばDES (Data Encryption Standard) や、AES (Advanced Encryption Standard) などの共通鍵暗号アルゴリズムや、RSAなどの公開鍵暗号アルゴリズムなどの種々の暗号アルゴリズムを適用可能である。適応した暗号アルゴリズムを特定する情報は、メインヘッダ、タイルパートヘッダ、或いは、パケットヘッダなどに記録して、後述する暗号復号処理部に送信するようにすればよい。また、後述する終端マーカの後に付与する付加情報の一部として送信しても良い。また、予め暗号復号処理部と復号処理部で共有するようにしておいても良い。

【0048】

次に、ステップS45では、暗号化対象のコードブロック*i*を、スクランブル再生モードとするか、或いは非スクランブル再生モードとするかが選択される。スクランブル再生モードの場合には処理をステップS46に進め、一方で非スクランブル再生モードの場合には処理をステップS47に進める。

【0049】

ここで、スクランブル再生モードと非スクランブル再生モードについて説明する。

【0050】

一般に、JPEG2000等の階層構造を有する画像データを再現するときには、低解像度の符号化データから高解像度の符号化に向かって復号処理を行っていく。従って、ウェーブレット変換を利用するJPEG2000の符号化データにおいて、LLを先ず復号し、その復号結果と {LH2+HH2+HL2} の符号化データとを利用して、更に高い解像度の画像を再現する。そしてその結果と {LH3+HH3+HL3} の符号化データとを利用して更に高い解像度のデー

タを再現し、最終的な復号結果となる。

【0 0 5 1】

ここで、 $\{LH3 + HH3 + HL3\}$ の符号化データが暗号化されていると仮定する。このとき、暗号化を解除する鍵情報を持たないとすると、 $\{LH2 + HH2 + HL2\}$ までは正常な像として再現できるものの、続く $\{LH3 + HH3 + HL3\}$ を利用したとたんに無意味なノイズが重畳した像が再現されてしまう。この再生モードを、実施形態ではスクランブル再生モードという。

【0 0 5 2】

一方、データとしては LL 、 $\{LH2 + HH2 + HL2\}$ が非暗号化され、 $\{LH3 + HH3 + HL3\}$ の符号化データが暗号化されている場合、復号処理を $\{LH2 + HH2 + HL2\}$ の符号化データに基づく復号処理で中止する再生モードを、実施形態では、非スクランブル再生モードという。

【0 0 5 3】

このスクランブル再生モードと非スクランブル再生モードについて、図 7 に示す例を用いて説明する。

【0 0 5 4】

図 7 (a) は 3 つの解像度レベル (ウェーブレット変換を 2 回行った場合) を有するコードストリームのウェーブレット変換領域を示す図である。また、ここでは、上記と同様、最高解像度レベルである $\{LH3, HH3, HL3\}$ に対応するパケットを暗号化し、それ以外の解像度レベルは暗号化しない例を示している。

【0 0 5 5】

同図 (b) は通常の復号化処理で再生した像を示し、 $\{LH3, HH3, HL3\}$ の暗号化された復号データを利用したために、画像にスクランブルされた状態を示している。また、同図 (c) は非スクランブル再生モードを適用することで、最高解像度である $\{LH3, HH3, HL3\}$ の暗号化データを利用せず、それより 1 段階前の解像度で処理を打ち切った場合の例を示している。同図 (c) は、最高解像度の画像とはならないので、多少のジャギーが発生するが、少なくとも同図 (a) よりは意味のある画像が再現できることになる。なお、暗号化

を解除する鍵情報を取得した場合、当然、 $\{LH3, HH3, HL3\}$ の暗号化を解除して、復号処理が継続することができるので、この場合には、同図 (d) に示すようになる。

【0056】

このように、スクランブル再生モードで処理した場合には、暗号化された解像度レベルは暗号化された状態で再生復号される。即ち、図7 (b) に示すように、最高解像度レベル以外（暗号化されていない解像度レベル）は正常に再生されるが、最高解像度レベルの packets (暗号化されている解像度レベル) はノイズとなって再生される。その結果、画像全体としては、いわゆるスクランブルされたような状態となって見える。

【0057】

一方、非スクランブル再生モードで処理した場合には、暗号化された解像度レベルは全く再生復号されない。即ち、図7 (c) に示すように、暗号化されていない中の最高解像度レベル（図示では $\{LH2 + HH2 + HL2\}$ ）まで正常に再生され、それより高い解像度の再現は行わない。その結果、画像全体としては、元の画像の解像度に比べて解像度が低い画像となって見えるものの、違和感のない再現が可能になる。

【0058】

上記解像度レベルに対する再生制御を行うための処理は、図4 のステップ S45 の判定で行われる。

【0059】

ステップ S46 に処理が進むと、終端マークが暗号化されたコードブロック i の後ろに付与される。一方、ステップ S47 では、終端マークが暗号化されたコードブロック i の前に付与される。

【0060】

ここで、終端マークについて説明する。本実施形態における終端マークとは、コードブロック内の符号列とコードブロック外の符号列の境界を表す特別なマークである。例えば、JPEG 2000 規格においては、 $0xFF90$ 以上の値を有する符号が終端マークに割り当てられている。このため、圧縮復号処理部では

終端マーカを受信すると、その後のコードブロック内のビットストリームは復号しないように設計されている。要するに、終端マーカ（終端情報）は、それより前のデータは意味のあるデータであるとし、それ以降は無意味なデータであるとするものである。本実施形態ではこれを利用することになる。

【0061】

終端マーカについて、更に、図5を用いて説明する。図5において51、及び53はビットストリーム、52は終端マーカを表す。図5に示したような状態の場合、後述する圧縮復号処理部はビットストリーム51は通常通り圧縮復号していくが、終端マーカ51を検出した場合、同じコードブロック中の後続するビットストリーム53は圧縮復号しない。

【0062】

本発明は、こうした終端マーカの性質を利用して、スクランブル再生モードの場合は終端マーカを暗号文の後ろに付与し、非スクランブル再生モードの場合は終端マーカを暗号文の前に付与するように処理するものである。即ち、スクランブル再生モードにおいては、暗号文は終端マーカの前に位置するためスクランブル状態として再生されるが、非スクランブル再生モードにおいては、暗号文は終端マーカの後に位置するため再生されない。

【0063】

図20で説明した、設定ウインドウ208における終端マーカの選択パラメータ「前」、「後」はかかる意味である。従って、図20におけるユーザが選択する項目を別な言い方をすれば、スクランブル再生モードにするか、非スクランブル再生モードにするか、でもある。

【0064】

また、本実施形態では終端マーカだけを付与するものとして説明したが、本発明はこれに限定されることなく、種々の付加情報を終端マーカの後に付与するようにしてもよい。例えば、当該コードブロックやパケットなどを復号する鍵に関連する情報（暗号化された鍵や、鍵へのポインタなど）や、暗号化のための各種パラメータ（ブロック暗号における利用モードなど）や、暗号化アルゴリズムに関連する情報（暗号化アルゴリズム名や暗号化アルゴリズムを特定する情報）な

どを付加するようにしても良い。

【0 0 6 5】

また、本実施の形態において、ステップ S 4 6、及びステップ S 4 7において終端マーカ（及び付加情報）を付与する方法については、終端マーカ（及び付加情報）を新たに追加しても良いし、暗号化された、又は、暗号化されていないビットストリームと置換するようにしても良い。終端マーカを付与する場合の例について更に図 6 を用いて説明する。

【0 0 6 6】

終端マーカを追加した場合の例を図 6（a）、及び（b）に示す。図 6（a）、及び（b）は暗号化されたパケットボディを示している。図 6 に示す例では、パケットは図中太線で示す 5 つのコードブロックから構成されている。また、図中網掛けした箇所は終端マーカを示す。すなわち、図 6（a）はスクランブル再生モードを示し、図 6（b）は非スクランブル再生モードを示すことになるのは、上記理由から明らかである。

【0 0 6 7】

図 6（a）、及び（b）に示すように、終端マーカを追加した場合には、暗号化の前後で追加した終端マーカの分だけコードブロックの長さが長くなる為に、パケットヘッダに記録されている各コードブロックの長さや、タイルパートヘッダに記録されているタイルパートの長さを適当な長さに修正する必要がある。

【0 0 6 8】

一方、終端マーカを置換した場合の例を図 6（c）、（d）に示す。図 6（c）及び（d）は、図 6（a）、及び（b）と同様に暗号化されたパケットボディを示している。図 6（c）、及び（d）に示す例でも、パケットは図中太線で示す 5 つのコードブロックから構成されている。また、図中網掛けした箇所は終端カーマを示す。即ち、図 6（c）はスクランブル再生モードを示し、図 6（d）は非スクランブル再生モードを示す。

【0 0 6 9】

図 6（c）、及び（d）に示すように、終端マーカを置換した場合には、暗号化の前後でコードブロックの長さが変化することはない。終端マーカを置換する

前のビットストリームの情報は、タイルパートヘッダやパケットヘッダなどに記録しておくようにすればよい。また、終端マーカを置換する前のビットストリームへ戻す為の鍵情報として、暗号化処理部から復号処理部に送信されるようにしても良い。

【0070】

尚、本実施形態では、ステップS45においてスクランブルモードが選択された場合、ステップS46において、終端マーカを暗号化したコードブロックiの後ろに付けるようにした。しかしながら本実施形態はこれに限定されることなく、スクランブルモードの場合には終端マーカを付けないようにすることも可能であることは明らかである。この場合、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダなどに当該コードブロック、或いはパケットが暗号化されていることを記録するようにすれば良い。

【0071】

また、本実施形態では、前述したように終端マーカの後に更に付加情報を付与することも可能である。図6(e)、及び(f)は、終端マーカの後にパケットに関する付加情報(図中、斜線で示す)を付与した場合の構成を示す。図6(e)はスクランブルモードにおけるパケットの構成を示し、図6(f)は非スクランブルモードにおけるパケットの構成を示す。図6(e)に示すように、スクランブルモードの場合は、パケットに関する付加情報は、パケットに含まれる最初のコードブロックの後だけに、終端マーカに続けて付加するようにすれば良い。一方、図6(f)に示すように、非スクランブルモードの場合は、パケットに関する付加情報は、パケットに含まれる最初のコードブロックの前に、終端マーカに続けて付加し、更に、最初のコードブロック以外の夫々のコードブロックの前には終端マーカだけを付加するようにすればよい。以上のような構成とすることによって、パケットに関する付加情報を(パケット中の全てのコードブロックに付与することなく)効率的に付与できる。

【0072】

次に、ステップS48では、パラメータiの値が1だけ増やされ、ステップS49でパラメータiとNの値が比較される。ここで、Nはパケットに含まれるコ

ードブロックの総数である。i がNより小さいときは処理をステップS43に進め、i がN以上の時にはパケット暗号化処理を終了する。

【0073】

尚、本実施の形態では、「暗号化されているか否か」という情報は終端マーカの直後に暗号化されていることを示す符号によって記録した。この場合、後述する暗号復号処理部において、パケットが暗号化されているか否かを確かめるためには、パケットの構造を解析して、コードブロック内の終端マーカの直後を調べる必要がある。しかしながら、本発明はこれに限定されることなく、終端マーカに加えて、メインヘッダ、タイルパートヘッダ、パケットヘッダの内部或いは外部において、パケットが暗号化されていることを示すような情報を記録するようにしてもよい。このようにすることによって、後述する暗号復号処理部において、パケットの構造を解析することなく、パケットが暗号化されているか否かを調べることが可能である。

【0074】

以上、本実施形態における暗号化処理部について説明した。

【0075】

<暗号復号処理部>

次に、図8を用いて本実施の形態における暗号復号処理機能を説明する。この処理は、図14における画像復号装置142における処理であると言えば分かりやすい。また、JPEG2000による復号処理は後段に位置することになる。図8の構成は、あくまで暗号を復号、すなわち、解除する処理機能を示していることに注意されたい。

【0076】

図8において、81はコードストリーム入力部、82はコードストリーム復号部、83はコードストリーム出力部である。

【0077】

コードストリーム入力部81はコードストリームを入力し、それに含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し、必要な場合は処理の流れを制御し、或いは後続の処理ユニットに対して該当するパラメータを送出する

ものである。通常は、前述した図 1 に示す暗号化処理部において暗号化処理されたコードストリーム C が入力される。しかしながら、暗号化が施されていないコードストリームが入力されても構わない。入力されたコードストリーム P はコードストリーム暗号化部 12 に出力される。

【0078】

コードストリーム復号部 82 はコードストリーム C を入力し、暗号復号鍵情報に従って（もし存在すれば）、コードストリーム C の所定の部分を復号処理し、復号処理されたコードストリーム P' が出力される。コードストリーム C に施されている全ての暗号が復号（暗号解除）される場合には、コードストリーム P' はコードストリーム P と等しいものになる。しかしながら、後述する種々の条件（復号鍵が存在しなかったり、明示的にスクランブル再生が指定された場合など）により、全ての暗号が復号されない場合には、コードストリーム P' はコードストリーム P と等しいものとはならない。コードストリーム復号処理部 82 で実行されるコードストリーム復号処理の詳細は後述する。復号されたコードストリーム C はコードストリーム出力部 83 に出力される。

【0079】

コードストリーム出力部 83 は、前段のコードストリーム復号処理部 82 で復号されたコードストリーム P' が入力され、復号されたコードストリーム P' が出力される。復号されたコードストリーム P' は、画像として再生するために、後述する圧縮復号処理部に出力される。

【0080】

次に、コードストリーム復号処理部 82 で実行されるコードストリーム復号処理について図 9 を用いて説明する。図 9 は本実施形態におけるコードストリーム復号処理を説明するフローチャートである。

【0081】

まず、入力されたコードストリーム C に対して、ステップ S91 では、メインヘッダ及びタイルパートヘッダが解析される。次に、ステップ S92 では、パラメータ j が 0 に初期化される。j はパケットを特定するパラメータである。続いて、ステップ S93 では、特定されたパケット j 内に暗号化されたコードブロッ

クがあるか否かが判定される。

【0082】

実施形態では、パケットを構成するコードブロック中の終端マーカの直後に暗号化されている／いないを示す情報を格納しているので、これを検出することで行うが、例えば、メインヘッダ、タイルパートヘッダ、パケットヘッダの内部或いは外部において、パケットが暗号化されていることを示す情報を調べることによって、判定しても構わない。これらの情報が用いられていない場合には、ステップS93による判定処理をスキップすることも可能である。

【0083】

ステップS94では、パケットjに対して、パケット復号処理が施される。パケット復号処理の詳細は後述する。また、ステップS95では、パラメータjの値が1だけ増やされ、ステップS95でパラメータjとMの値が比較される。ここで、Mはコードストリームに含まれるパケットの総数である。jがMより小さいときは処理をステップS93に進め、jがM以上の時にはコードストリーム復号処理を終了する。

【0084】

次に、本実施形態におけるパケット復号処理の詳細について、図10を用いて説明する。この処理は、注目パケット内に暗号化されたコードブロックが存在すると判定された場合である。

【0085】

まず、入力されたパケットjに対して、ステップS101では、パケットjのパケットヘッダが解析され、当該パケットに含まれるコードブロック等の構造が解析される。その後、ステップS102では、パラメータiが0に初期化される。パラメータiはコードブロックを特定するパラメータである。

【0086】

続いて、ステップS103では、特定されたコードブロックiが暗号化されているか否かが判定される。この判断は、先に説明したように、終端マーカの直後に暗号化されていることを示す情報があるか否かで判断するが、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダ内に、暗号化されている箇所を明記

する情報を格納しておき、これによって判断しても構わない。

【0087】

暗号化されていないと判断した場合には、ステップS107に進み、注目コードブロックはそのままの状態で出力され、変数*i*を1つ増加させ、上記ステップS103以降の処理（次のコードブロックに対する処理）を行う。

【0088】

さて、コードブロック*j*が暗号化されていると判断した場合、処理はステップS104に進み、暗号化を解除する鍵情報が存在するか否かを判断する。

【0089】

もし、その鍵情報が存在しないと判断した場合には、ステップS107に移って、そのままの状態の後段の処理に渡すことになる。従って、終端マークがコードブロックの先頭にある場合には、そのまま後段に出力され、終端マーク以降、すなわち、注目コードブロックについては符号化データの復号処理が行われなくなるので、非スクランブル再生が行われることになる。また、終端マークがコードブロックの後端にある場合には、暗号化されたままの状態で符号化データを復号してしまうので、スクランブル再生が行われることになる（この場合には、終端マークを削除しても構わない）。

【0090】

さて、ステップS104において、暗号を解除する鍵情報が存在すると判断した場合、処理はステップS106に進む。ここでは、注目の暗号化されたコードブロックを、その鍵情報に従って復号する。このとき、終端マークがコードブロックの先頭にあった場合には、その後端に移動させる（削除でも良い）。更に、メインヘッダ、タイトルパートヘッダ、或いはパケットヘッダに、当該コードブロックが暗号化されている情報が記録されている場合には、これらの情報を暗号化されていないことを表すように変更する。

【0091】

この後、処理はステップS107に進み、暗号解除毎のコードブロックを出力し、変数*i*を更新することになる。

【0092】

以上の処理を、ステップ S 1 0 8 で注目パケットに含まれる全コードブロックに対して行ない、その処理を終えた場合には図 9 のステップ S 9 5 に復帰し、次のパケットに対する処理を行うことになる。

【 0 0 9 3 】

以上、本実施形態における暗号復号処理部について説明した。

【 0 0 9 4 】

上記処理を行うと、暗号化を解除する鍵情報が存在しない場合、各パケットを構成するコードブロックの終端マークは、入力したストリームのまま維持されることになる。換言すれば、暗号化したユーザの意図が反映された状態で、符号化画像データの復号処理が行われることになる。

【 0 0 9 5 】

一方、暗号化を解除する鍵情報が存在した場合には、暗号化されたコードブロックのデータの暗号化が解除され、尚且つ、終端マークがコードブロックの後端に位置する、もしくは削除されることになり、そのコードブロックを利用した再現処理が行われることになる。

【 0 0 9 6 】

< 圧縮符号化処理部 >

以上であるが、実施形態における装置 1 4 1 は、既に J P E G 2 0 0 0 で圧縮符号化された画像ファイルを暗号化する例を説明したが、生の画像データを符号化し、それに後続する処理として図 1 の構成を設けても構わない。

【 0 0 9 7 】

従って、かかる構成にした場合の画像圧縮符号化について説明することとする。

【 0 0 9 8 】

まずはじめに、図 1 1 を用いて本実施形態における圧縮符号化処理を説明する。

【 0 0 9 9 】

図 1 1 において、1 1 1 は画像入力部、1 1 2 は離散ウェーブレット変換部、1 1 3 は量子化部、1 1 4 はエントロピ符号化部、1 1 5 は符号出力部である。

まず、画像入力部 111 に対して符号化対象となる画像を構成する画素信号がラスタースキャン順に入力し、その出力は離散ウェーブレット変換部 112 に入力される。以降の説明では、その説明を容易なものとするため、画像信号はモノクロの多値画像を表現しているが、カラー画像等、複数の色成分を符号化するならば、RGB 各色成分、或いは輝度、色度成分を上記単色成分として圧縮すればよい。

【0100】

離散ウェーブレット変換部 112 は、入力した画像信号に対して 2 次元の離散ウェーブレット変換処理を行い、変換係数を計算して出力するものである。図 12 (a) は離散ウェーブレット変換部 12 の基本構成を表したものであり、入力された画像信号はメモリ 121 に記憶され、処理部 122 により順次読み出されて変換処理が行われ、再びメモリ 121 に書きこまれており、本実施の形態においては、処理部 122 における処理の構成は同図 (b) に示すものとする。同図において、入力された画像信号は遅延素子およびダウンサンプラの組み合わせにより、偶数アドレスおよび奇数アドレスの信号に分離され、2 つのフィルタ p および u によりフィルタ処理が施される。同図 s および d は、各々 1 次元の画像信号に対して 1 レベルの分解を行った際のローパス係数およびハイパス係数を表しており、次式により計算されるものとする。

$$d(n) = x(2*n + 1) - \text{floor}((x(2*n) + x(2*n + 2))/2) \quad (\text{式 1})$$

$$s(n) = x(2*n) + \text{floor}((d(n - 1) + d(n))/4) \quad (\text{式 2})$$

ただし、 $x(n)$ は変換対象となる画像信号であり、 $\text{floor}(x)$ は x を越えない最大整数を返す関数である。

【0101】

以上の処理により、画像信号に対する 1 次元の離散ウェーブレット変換処理が行われる。2 次元の離散ウェーブレット変換は、1 次元の変換を画像の水平・垂直方向に対して順次行うものであり、その詳細は公知であるのでここでは説明を省略する。図 12 (c) は 2 次元の変換処理により得られる 2 レベルの変換係数群の構成例であり、画像信号は異なる周波数帯域の係数列 HH1、HL1、LH1、…、LL に分解される。なお、以降の説明ではこれらの係数列をサブバンド

と呼ぶ。また、同じ分割レベルに属するサブバンドの集合を解像度レベルと呼ぶ。例えば、HH 1、HL 1、LH 1は同じ解像度レベルに属する。各サブバンドの係数は後続の量子化部 1 1 3 に出力される。

【0 1 0 2】

量子化部 1 1 3 は、入力した係数を所定の量子化ステップにより量子化し、その量子化値に対するインデックスを出力する。ここで、量子化は次式により行われる。

$$q = \text{sign}(c) \text{ floor}(\text{abs}(c) / \Delta) \quad (\text{式 3})$$

$$\text{sign}(c) = 1; c \geq 0 \quad (\text{式 4})$$

$$\text{sign}(c) = -1; c < 0 \quad (\text{式 5})$$

ここで、 c は量子化対象となる係数である。

【0 1 0 3】

また、本実施の形態においては Δ の値として1を含むものとする。この場合実際に量子化は行われず、量子化部 1 1 3 に入力された変換係数はそのまま後続のエントロピ符号化部 1 1 4 に出力される。

【0 1 0 4】

エントロピ符号化部 1 1 4 は入力したサブバンドを互いに重ならない複数の矩形領域に分割し、夫々の分割した矩形領域に含まれる量子化インデックスをビットプレーンに分解し、ビットプレーンを単位として2値算術符号化を行ってコードストリームを出力する。ここで、エントロピ符号化部における符号化単位となる矩形領域をコードブロックと呼ぶ。

【0 1 0 5】

図 1 3 はエントロピ符号化部 1 4 の動作を説明する図であり、この例においては 4×4 の大きさを持つコードブロックにおいて非0の量子化インデックスが3個存在しており、それぞれ+13、-6、+3の値を持っている。エントロピ符号化部 1 4 はコードブロックを走査して最大値MAXを求め、次式により最大の量子化インデックスを表現するために必要なビット数Sを計算する。

$$S = \text{ceil}(\log_2(\text{abs}(\text{MAX}))) \quad (\text{式 6})$$

ここで $\text{ceil}(x)$ は x 以上の整数の中で最も小さい整数値を表す関数であ

る。

【0106】

図13においては、最大の係数値は13であるのでSは4であり、シーケンス中の16個の量子化インデックスは同図(b)に示すように4つのビットプレーンを単位として処理が行われる。最初にエントロピ符号化部114は最上位ビットプレーン(同図MSBで表す)の各ビットをエントロピ符号化(本実施の形態では2値算術符号化)し、ビットストリームとして出力する。次にビットプレーンを1レベル下げ、以下同様に対象ビットプレーンが最下位ビットプレーン(同図LSBで表す)に至るまで、ビットプレーン内の各ビットを符号化し符号出力部15に出力する。なお上記エントロピ符号化時において、各量子化インデックスの符号は、上位から下位へのビットプレーン走査において最初(最上位)に符号化されるべき非0ビットが検出されるとそのすぐ後に当該量子化インデックスの正負符号を示す1ビットを続けて2値算術符号化することとする。これにより、0以外の量子化インデックスの正負符号は効率良く符号化される。

【0107】

尚、以上の様にエントロピ符号化されたエントロピ符号を所定の符号量となるように集めた処理単位をレイヤと呼ぶ。複数のレイヤを構成することにより、復号時に種々の符号量に対応した画像を再生することが可能となる。

【0108】

また、最上位のビットプレーンの情報が各値に支配的であることに注意されたい。つまり、先に説明した例では、ウェーブレット変換する際のサブバンド、もしくは周波数成分グループに対して暗号化する／しないを設定したが、上記の如く、各ビットプレーンのどのレベルについて暗号化する／しないを設定したとしても同様の効果が期待できる。例えば、最下位(ビット0)のビットプレーンに対して暗号化を行えば、それより1つ上位(ビット1)のプレーンまでの復号化でもって再生される画像は、最高解像度よりも1つ下の解像度となって再現できることになり、図7とほぼ等価の状態となる。

【0109】

<圧縮復号処理部>

次に以上述べた圧縮符号化処理部による符号列を復号する方法について説明する。

【0110】

図15は本実施の形態における圧縮復号化処理部の構成を表すブロック図であり、151が符号入力部、152はエントロピ復号部、153は逆量子化部、154は逆離散ウェーブレット変換部、155は画像出力部である。

【0111】

符号入力部151は符号列を入力し、それに含まれるヘッダを解析して後続の処理に必要なパラメータを抽出し必要な場合は処理の流れを制御し、あるいは後続の処理ユニットに対して該当するパラメータを送出するものである。図8に示すコードストリーム出力部83からの出力を、入力すると言えばわかり易い。また、符号列に含まれるビットストリームはエントロピ復号部152に出力される。

【0112】

エントロピ復号部152はビットストリームをコードブロックに分割し、コードブロック内においてビットプレーン単位で復号し、出力する。この時の復号化手順を図16に示す。図16(a)は復号対象となるコードブロックをビットプレーン単位で順次復号化し、最終的に量子化インデックスを復元する流れを図示したものであり、同図の矢印の順にビットプレーンが復号される。復元された量子化インデックスは逆量子化部153に出力される。

【0113】

次に、逆量子化部153は入力した量子化インデックスから、次式に基づいて離散ウェーブレット変換係数を復元する。

$$c' = \Delta * q; \quad q \neq 0 \quad (\text{式7})$$

$$c' = 0; \quad q = 0 \quad (\text{式8})$$

ここで、 q は量子化インデックス、 Δ は量子化ステップであり、 Δ は符号化時に用いられたものと同じ値である。 c' は復元された変換係数であり、符号化時では s または d で表される係数の復元したものである。変換係数 c' は後続の逆離散ウェーブレット変換部154に出力される。

【0114】

図17は逆離散ウェーブレット変換部154の構成および処理のブロック図を示したものである。同図(a)において、入力された変換係数はメモリ171に記憶される。処理部172は1次元の逆離散ウェーブレット変換を行い、メモリ171から順次変換係数を読み出して処理を行うことで、2次元の逆離散ウェーブレット変換を実行する。2次元の逆離散ウェーブレット変換は、順変換と逆の順序により実行されるが、詳細は公知であるので説明を省略する。また同図(b)は処理部172処理ブロックを示したものであり、入力された変換係数はuおよびpの2つのフィルタ処理を施され、アップサンプリングされた後に重ね合わされて画像信号x'が出力される。これらの処理は次式により行われる。

$$x'(2*n) = s'(n) - \text{floor}((d'(n-1) + d'(n))/4) \quad (\text{式9})$$

$$x'(2*n+1) = d'(n) + \text{floor}((x'(2*n) + x'(2*n+2))/2) \quad (\text{式10})$$

ここで、式(1)、式(2)、および式(9)、式(10)による順方向および逆方向の離散ウェーブレット変換は完全再構成条件を満たしているため、本実施形態において量子化ステップΔが1であり、ビットプレーン復号において全てのビットプレーンが復号されていれば、復元された画像信号x'は原画像の信号xと一致する。

【0115】

以上の処理により画像が復元されて画像出力部155に出力される。画像出力部155はモニタ等の画像表示装置であってもよいし、あるいは磁気ディスク等の記憶装置であってもよい。

【0116】

<第1の実施形態の変形例>

上記実施形態では、例えば、図7の如く、{LH3+HH3+HL3}について暗号化され、それ以外では非暗号化の符号化データを装置142が受信し再生するときであって、その装置142が暗号解除鍵情報を持たない場合には、上記最高解像度に相当するデータが暗号化されたまま再生することになり、結果的に、図7(b)に示すようなスクランブルされた画像が表示されてしまう。

【0117】

しかしながら、もともと暗号化する側である装置 141 のユーザは、 $\{LH2 + HH2 + HL2\}$ までの、最高解像度よりも 1 つ手前までの再生を許容しているわけであるから、装置 142 のユーザが仮に暗号化を解除する鍵情報を所有していなくても、必要に応じて $\{LH3 + HH3 + HL3\}$ のデータを利用する直前までの状態で再現できるようにすることが望まれる。

【0118】

そこで、本第 1 の実施形態における変形例では、この問題を解決する。

【0119】

図 10B は、先に説明した図 10A に置き換わるものである。それ以外の装置構成は第 1 の実施形態と同様であるものとし、以下では、図 10B について説明することとする。

【0120】

図 10B において、図 10A と異なる点は、ステップ S105、109、110 が追加された点であるが、以下、順に説明することとする。なお、以下の処理をはじめるとあって、装置 142 のユーザは、スクランブルを解除するか否かを設定しているとする。この設定は、暗号化解除する際に適宜設定しても良いし、予め、そのユーザの設定事項をファイル等に記憶保持しておくようにしてもよい。前者の場合には、個々の画像を再生する際に、その都度行えることになり、後者の場合には特に変更しない限りは、その設定内容が全ての画像復号に反映されることになる。

【0121】

まず、入力されたパケット j に対して、ステップ S101 では、パケット j のパケットヘッダが解析され、当該パケットに含まれるコードブロック等の構造が解析される。その後、ステップ S102 では、パラメータ i が 0 に初期化される。パラメータ i はコードブロックを特定するパラメータである。

【0122】

続いて、ステップ S103 では、特定されたコードブロック i が暗号化されているか否かが判定される。この判断は、先に説明したように、終端マーカの直後に暗号化されていることを示す情報があるか否かで判断するが、メインヘッダ、

タイルパートヘッダ、或いはパケットヘッダ内に、暗号化されている箇所を明記する情報を格納しておき、これによって判断しても構わない。

【0123】

暗号化されていないと判断した場合には、ステップS107に進み、注目コードブロックはそのままの状態出力され、変数*i*を1つ増加させ、上記ステップS103以降の処理（次のコードブロックに対する処理）を行う。

【0124】

また、コードブロック*j*が暗号化されていると判断した場合、処理はステップS104に進み、暗号化を解除する鍵情報が存在するか否かを判断する。

【0125】

もし、その鍵情報が存在しないと判断した場合には、ステップS109に分岐し、鍵情報が存在すると判断した場合には、ステップS105に進むことになる。

【0126】

ステップS105では、所定のコードブロックをスクランブル再生するか、或いは非スクランブル再生するかが判定される。これは先に説明したように、装置142のユーザの設定内容によって判断することになる。通常、復号鍵を有している場合は非スクランブル再生することが多い。しかしながら、暗号化されているコードストリームの一部だけを復号し、一部の暗号文を復号しない場合などに、ステップS105により明示的にスクランブル再生を選択することが可能である。尚、復号鍵を有する全ての暗号文を復号する場合には、ステップS105は省略可能であることは明らかである。

【0127】

そして、ステップS106に進むと、コードブロック*i*が暗号の復号処理（暗号解除処理）される。暗号復号処理は、前述した図4におけるステップS44で用いた暗号アルゴリズムに対応したものでなければならない。ステップS44で用いた暗号アルゴリズムは、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダに記録してある情報を調べることにより知ることができる。また、前述したする終端マーカの後に付与されている付加情報を調べるようにしても良い。

また、暗号復号処理が施されたコードブロック内の終端マークはコードブロックの終端に位置させるか、或いは、除去する。更に、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダに、当該コードブロックが暗号化されている情報が記録されている場合には、これらの情報を暗号化されていないことを表すように変更する。

【0128】

一方、ステップS104で暗号を解除する鍵情報がないと判断した場合、処理はステップS109に進むことになる。このステップS109では、復号鍵がない場合に、非スクランブル再生するか否かが判定される。この判定は、ステップS105と同様であり、ユーザによって明示的に指示するようにしても良いし、予めRAMやHDDに記憶されている情報を用いて判定するようにしても良い。そして、非スクランブル再生する場合にはステップS110に進み、スクランブル再生する場合にはステップS107に進む。ステップS110では、終端マークが暗号文の前に付与されている場合には暗号文の後ろに移動させる。或いは、終端マークを消去するようにしても構わない。

【0129】

ステップS109、及びステップS110における処理について説明する。前述した暗号化処理部において、非スクランブル再生モードとした場合には、コードブロックi内において暗号文の前に終端マークが付加されている。これにより、当該終端マークにより暗号文を復号しないために、通常は非スクランブル再生モードとなる。しかしながら、本実施形態によれば判定処理S109により、スクランブル再生とするか非スクランブル再生とするかを選択することが可能となる。

【0130】

処理が、ステップS107に進むと、そのコードブロックを出力し、変数iをインクリメントし、ステップS108で注目パケットに含まれる全コードブロックに対して行なったか否かを判断し、否の場合には、ステップS103以降の処理を繰り返す。また、注目パケットの全コードブロックに対する処理が終了したと判断した場合には、図9のステップS95に復帰し、次のパケットに対する処

理を行うことになる。

【0131】

以上の結果、この変形例によれば、暗号化を解除する鍵情報を有しなくても、暗号化したユーザが認めた最高解像度レベルでの非スクランブル再生が行えるようになり、少なくともオリジナル画像そのものとはいかないまでも、許容された範囲内で最高画質を閲覧することが可能になる。

【0132】

なお、上記例では、暗号化されているか否かは、終端マーカの直後に、暗号化されているか否かの情報を付加し、それを識別することで行うものとして説明したが、J P E G 2 0 0 0では、通常、終端マーカを使うことが少ない。従って、終端マーカが存在するか否かで判定するようにしてもよい。この場合、終端マーカが存在すれば、暗号化が行われ、尚且つ、非スクランブル再生モードが設定されると見なすことになるであろう。

【0133】

<第2の実施形態>

上記実施形態（第1の実施形態及びその変形例）においては、図4に示したように暗号化をコードブロック単位で行うようにしたが、本発明はこれに限定されることなく、入力されたコードストリームを構成する種々の論理単位毎や、階層構造毎に暗号化をするようにすることも可能であることは明らかである。

【0134】

ここで、論理単位としては、パケット、タイルパート、タイル、コードストリーム、及びこれらの組み合わせなどを適応可能である。また、階層構造としては、解像度レベル、レイヤ、プレシント、コンポーネント、及びこれらの組み合わせなどを適応可能である。更に、階層構造毎に暗号化が施された場合には、メインヘッダ、タイルパートヘッダ、或いはパケットヘッダなどに、「どの階層構造が暗号されているか」ということを特定する情報を記録するようにしておく。

【0135】

これらの論理単位や階層構造ごとに暗号化が施された場合でも、第1の実施形態に示したように、非スクランブル再生モードの場合は、暗号化が施された論理

単位や階層構造に含まれる全てのコードブロック内の暗号文の前に終端マーカを付与するようにすることによって、非スクランブル再生モードとすることが可能である。

【0136】

また、前述したように、論理単位毎や階層構造毎に暗号化を施した場合には、当該暗号化されている論理単位や階層構造を特定し、特定された論理単位や解像構造の暗号を復号するようにすればよい。

【0137】

<第3の実施形態>

上記第1、第2の実施形態においては、図1に示したように暗号化処理部への入力には既に圧縮符号化された後のコードストリームであった。これは、圧縮符号化処理の実行と暗号化処理の実行を夫々独立な処理とし、一旦、圧縮符号化処理を実行した後に暗号化処理を実行するような構成とするものである。つまり、画像圧縮符号化は既存のアプリケーション等で行い、暗号化処理をそれとは独立したものとするのに都合が良い。

【0138】

同様に、図8に示したように暗号復号部からの出力もコードストリームであった。これは、暗号復号処理と圧縮復号処理とをそれぞれ独立にし、圧縮復号を取りを既存のアプリケーションで行うのに都合が良いものと言える。

【0139】

しかしながら本発明はこれに限定されることなく、圧縮符号化処理と暗号化処理とを同じアプリケーションとして実行、或いは、暗号符号化処理と圧縮復号処理を同じアプリケーションとして実行するような構成とすることも可能である。

【0140】

まずはじめに、図18を用いて本実施の形態における画像圧縮処理と暗号化処理部の構成を説明する。

【0141】

図18において、181は画像発生部（CCDスキャナやデジタルカメラ等のデバイスから画像データ入力するユニット）、182は離散ウェーブレット変換

部、183は量子化部、184はエントロピ符号化部、185は暗号化部、186はコードストリーム出力部である。

【0142】

画像発生部181、離散ウェーブレット変換部182、量子化部183、エントロピ符号化部184、及びコードストリーム出力部186の動作は、夫々、前述した図11における、画像発生部111、離散ウェーブレット変換部112、量子化部113、エントロピ符号化部114、及びコードストリーム出力部115の動作と同様の動作であるので詳細な説明は省略する。ただし、ウェーブレット変換する多少のタイル数、変換回数、量子化部での量子化ステップ等がユーザーの設定に応じて処理される。

【0143】

本実施形態では、エントロピ符号化部184においてエントロピ復号されたビットストリームに対して、暗号化部185において暗号化処理が実行される。暗号化処理の対象は第2の実施形態に示したように、種々の論理単位や階層構造に対応するビットストリームを選択可能である。また、非スクランブル再生モードの場合には、当該暗号化された論理単位や階層構造に含まれる全てのコードブロック内の暗号文の前に終端マーカを付与するようにすることによって、非スクランブル再生モードとすることが可能である。

【0144】

尚、本実施形態ではエントロピ符号化部184の後に暗号化部185が続く構成例を説明した。これは、暗号化部185でエントロピ復号されたビットストリームを暗号化の対象とするものである。しかしながら、本発明はこれに限定されることなく、量子化部183、離散ウェーブレット変換部182、或いは画像発生部181の後に暗号化部185が続く構成とすることも可能であることは明らかである。

【0145】

暗号化部185が量子化部183の後に続く場合には量子化インデックス（或いは、量子化インデックスを構成するビット列）が暗号化対象となる。また、離散ウェーブレット変換部182の後に続く場合には離散ウェーブレット変換係数

(或いは、離散ウェーブレット変換係数を構成するビット列) が暗号化対象となる。更に、画像発生部 181 の後に続く場合には画素 (或いは、画素を構成するビット列) が暗号化対象となる。

【0146】

なお、上記の処理を行う場合、生の画像データ (非圧縮の画像データ) を指定することになるので、暗号化対象ファイルは非圧縮の画像 (例えば拡張子が BMP) が選択可能になる。従って、この場合の GUI の例は、図 21 のようになる。また、また、JPEG2000 では、1 つの画像に対して複数のタイルを設定できるので、図 20 の画面にはタイル数の設定の入力欄 $\square \times \square$ (デフォルトで $1 \times 1 = 1$ 画像 1 タイル) を設け、更に、ウェーブレット変換回数をユーザが指定できるようにする。

【0147】

図 21 の場合、タイル数を 2×2 としているので、先ず、タイルを選択し、その中で暗号化対象を第 1 の実施形態と同様に設定することになる。なお、タイルそのものをも圧縮させることも可能であるので、図示の設定ウインドウ 208 には、タイル全体 (2×2 の 1 つ) について暗号化させることも可能とした。従って、オリジナル画像中の所望とする位置の、所望とする解像度について暗号化させることも可能となる。

【0148】

次に、図 19 を用いて本実施形態における暗号復号処理部の構成を説明する。

【0149】

図 19 において、191 はコードストリーム入力部、192 は暗号復号部、193 はエントロピ復号部、194 は逆量子化部、195 は逆離散ウェーブレット変換部、196 は画像データ出力部である。

【0150】

コードストリーム入力部 191、エントロピ復号部 193、逆量子化部 194、逆離散ウェーブレット変換部 195、及び画像データ出力部 196 の動作は、夫々、前述した図 15 における、コードストリーム入力部 151、エントロピ復号部 152、逆量子化部 153、逆離散ウェーブレット変換部 154、及び画像

出力部 155 と同様の動作であるので詳細な説明は省略する。

【0151】

本実施形態では、コードストリーム入力部 191 において入力されたビットストリームに対して、暗号復号部 192 において暗号復号処理が実行される。暗号復号処理の対象は第 2 の実施形態に示したように、種々の論理単位や階層構造に対応するビットストリームである。

【0152】

尚、本実施形態ではコードストリーム入力部 191 の後に暗号復号部 192 が続く構成例を説明した。これは、暗号復号部 192 で入力された暗号化されたビットストリームを暗号復号の対象とするものである。しかしながら、本発明はこれに限定されることなく、エントロピ復号部 193、逆量子化部 194、逆離散ウェーブレット変換部 195 の後に暗号復号部 192 が続く構成とすることも可能であることは明らかである。

【0153】

暗号復号部 192 がエントロピ復号部 193 の後に続く場合には暗号化された量子化インデックス（或いは、量子化インデックスを構成するビット列）が暗号復号の対象となる。また、逆量子化部 194 の後に続く場合には暗号化された離散ウェーブレット変換係数（或いは、離散ウェーブレット変換係数を構成するビット列）が暗号復号の対象となる。更に、逆離散ウェーブレット変換部 195 の後に続く場合には暗号化された画素（或いは、画素を構成するビット列）が暗号復号の対象となる。

【0154】

以上、本発明に係る実施形態を説明した。実施形態では、J P E G 2 0 0 0 を例にして説明したが、上記実施形態で説明した終端マーカ或いはそれと等価の意味を持つ終端情報を有する画像データであれば適用可能なので、上記実施形態で本願発明が限定されるものではない。また、暗号化対象は伝送効率の点で圧縮符号化されていて、尚且つ、階層構造を持つ、或いは、それに類する圧縮符号化データ（例えば J P E G）等であることが望ましいが、これは好適な例であって、必須のものではない。

【 0 1 5 5 】

また、実施形態での説明から明らかなように、装置 1 4 1、1 4 2 はパーソナルコンピュータ等の汎用情報処理装置上で動作するプログラムでもって実現できるわけであるから、本願発明はかかるコンピュータプログラムをもその範疇するのは明らかである。更にまた、通常コンピュータプログラムは、CDROM等のコンピュータ可読記憶媒体に記録され、それをコンピュータにセットすることで、システムにコピーもしくはインストールすることで実行可能になるわけであるから、本発明はかかるコンピュータ可読記憶媒体をもその範疇とするのは明らかである。

【 0 1 5 6 】**【発明の効果】**

以上説明したように本発明によれば、画像再生装置でスクランブルさせて再生させるか、或いは、非スクランブル状態で再生させるかを暗号化する側で設定可能となる。

【図面の簡単な説明】**【図 1】**

実施形態における暗号化処理部の構成を示す図である。

【図 2】

図 1 におけるコードストリーム暗号化部の処理手順を示すフローチャートである。

【図 3】

実施形態におけるコードストリームのデータフォーマットを示す図である。

【図 4】

図 2 におけるパケット暗号化処理の詳細を示すフローチャートである。

【図 5】

終端マーカの配置位置の一例を示す図である。

【図 6】

実施形態における暗号化後のコードブロックのデータフォーマットを示す図である。

【図 7】

実施形態における暗号化処理と、その再生例との対応関係を示す図である。

【図 8】

実施形態における暗号復号処理部の構成を示す図である。

【図 9】

図 8 におけるコードストリーム暗号復号処理部の処理手順を示すフローチャートである。

【図 10 A】

図 9 におけるパケット復号処理の処理手順の詳細を示すフローチャートである。

【図 10 B】

図 9 におけるパケット復号処理の他の処理手順の詳細を示すフローチャートである。

【図 11】

実施形態における画像圧縮符号化処理を行う際の構成を示す図である。

【図 12】

図 11 における離散ウェーブレット変換部の構成とその動作を説明するための図である。

【図 13】

図 11 におけるエントロピー符号化部の処理内容を説明するための図である。

【図 14】

実施形態におけるシステム全体の構成を示す図である。

【図 15】

実施形態における圧縮符号化データの復号処理を行う際の構成を示す図である。

【図 16】

図 15 におけるエントロピー復号部の処理内容を説明するための図である。

【図 17】

図 15 における逆離散ウェーブレット変換部の構成とその動作を説明するため

の図である。

【図 1 8】

第 3 の実施形態における画像圧縮・暗号化装置のブロック構成図である。

【図 1 9】

第 3 の実施形態における暗号復号・圧縮画像復号装置のブロック構成図である。

【図 2 0】

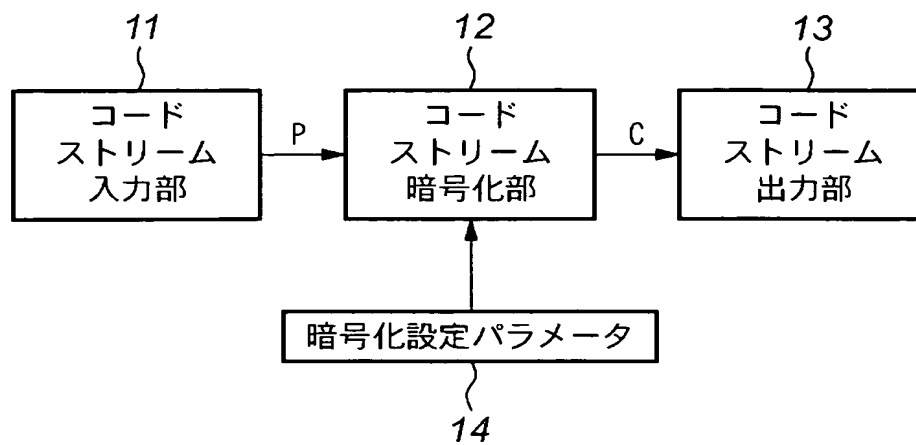
実施形態における暗号化処理におけるユーザインタフェースとなる設定ウインドウの一例を示す図である。

【図 2 1】

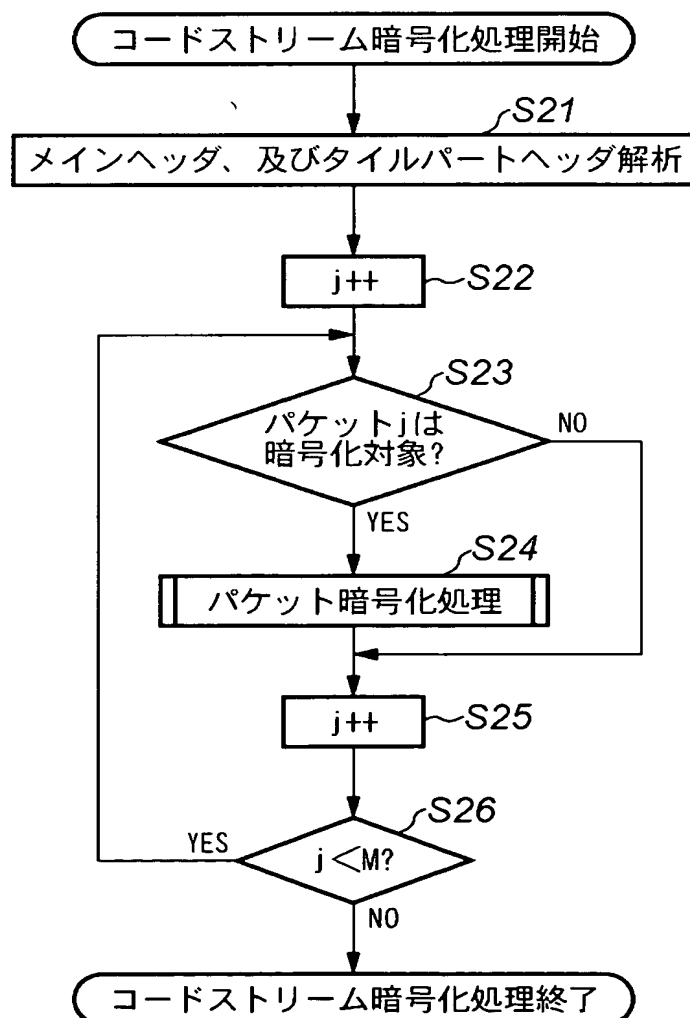
第 3 の実施形態における暗号化処理におけるユーザインタフェースとなる設定ウインドウの一例を示す図である。

【書類名】 図面

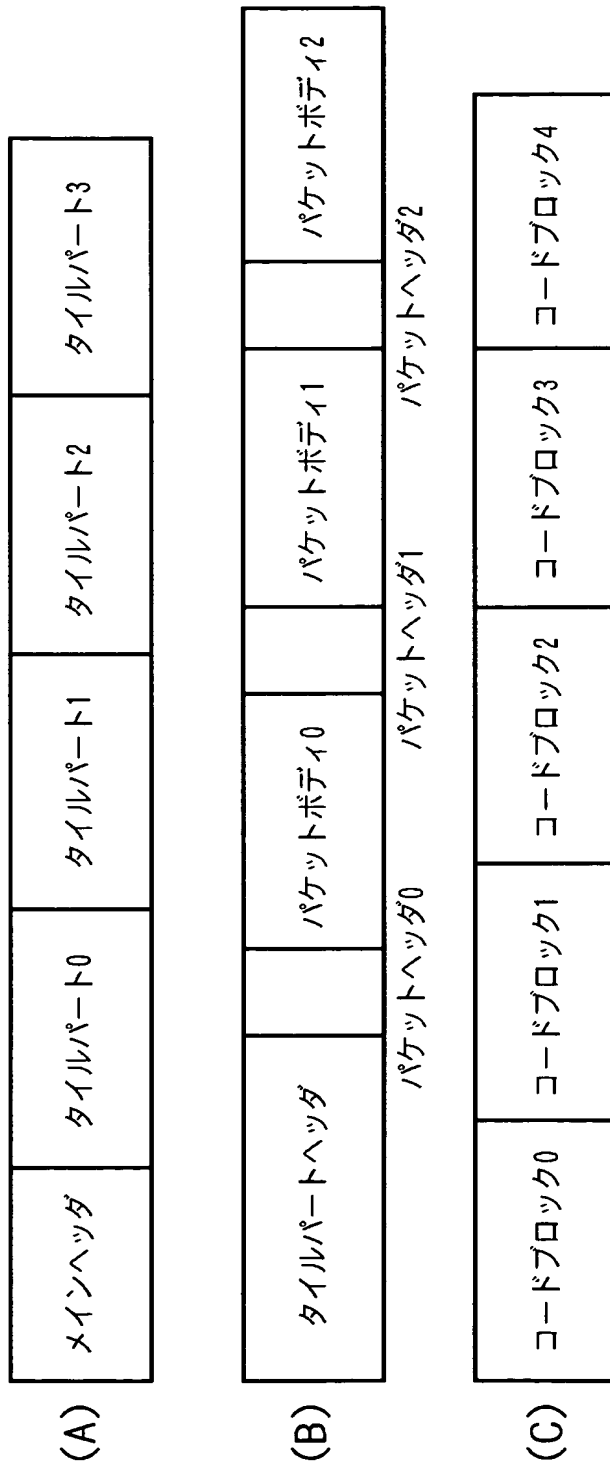
【図 1】



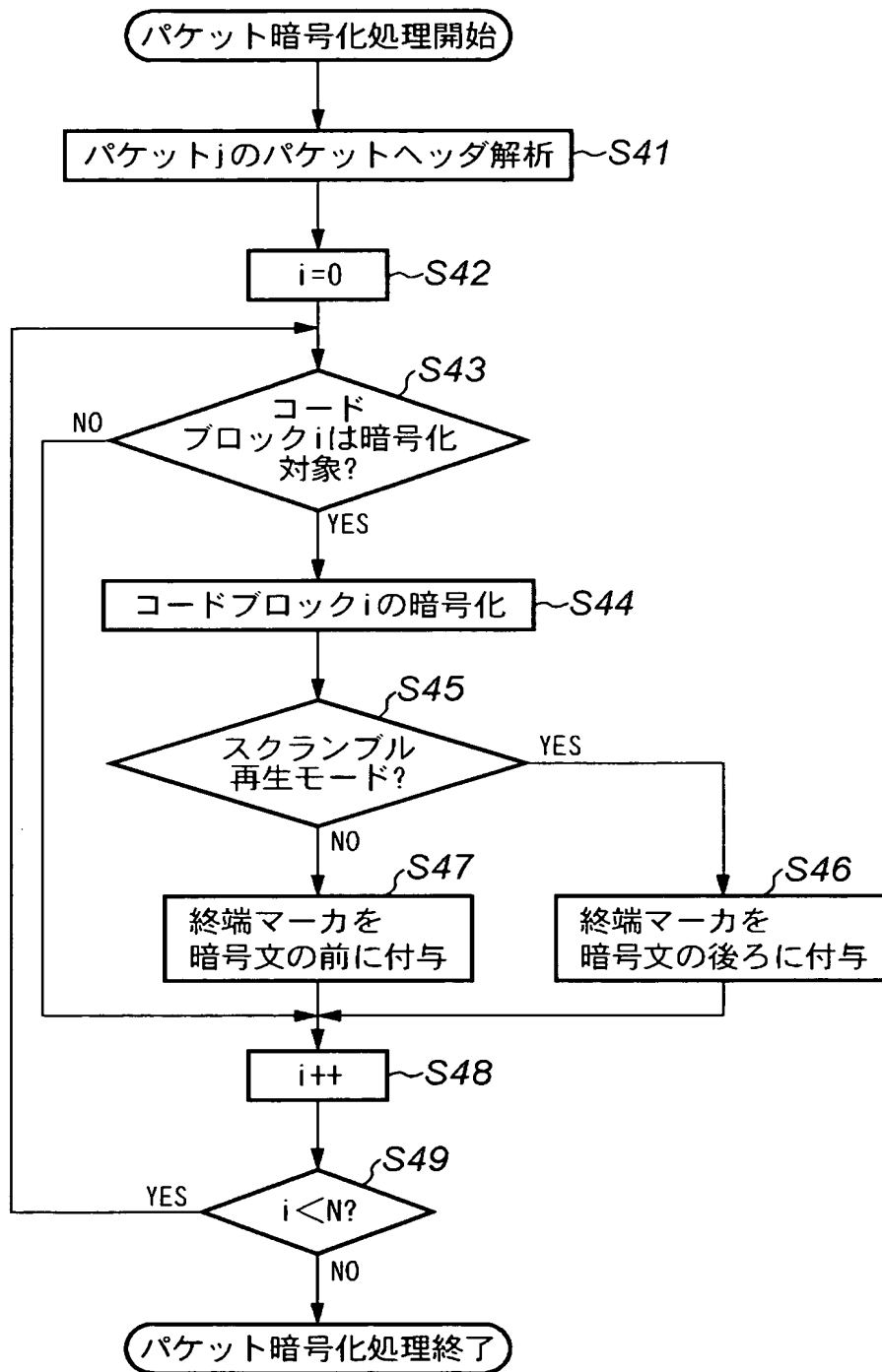
【図 2】



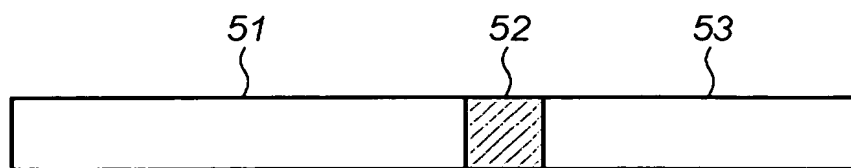
【図 3】



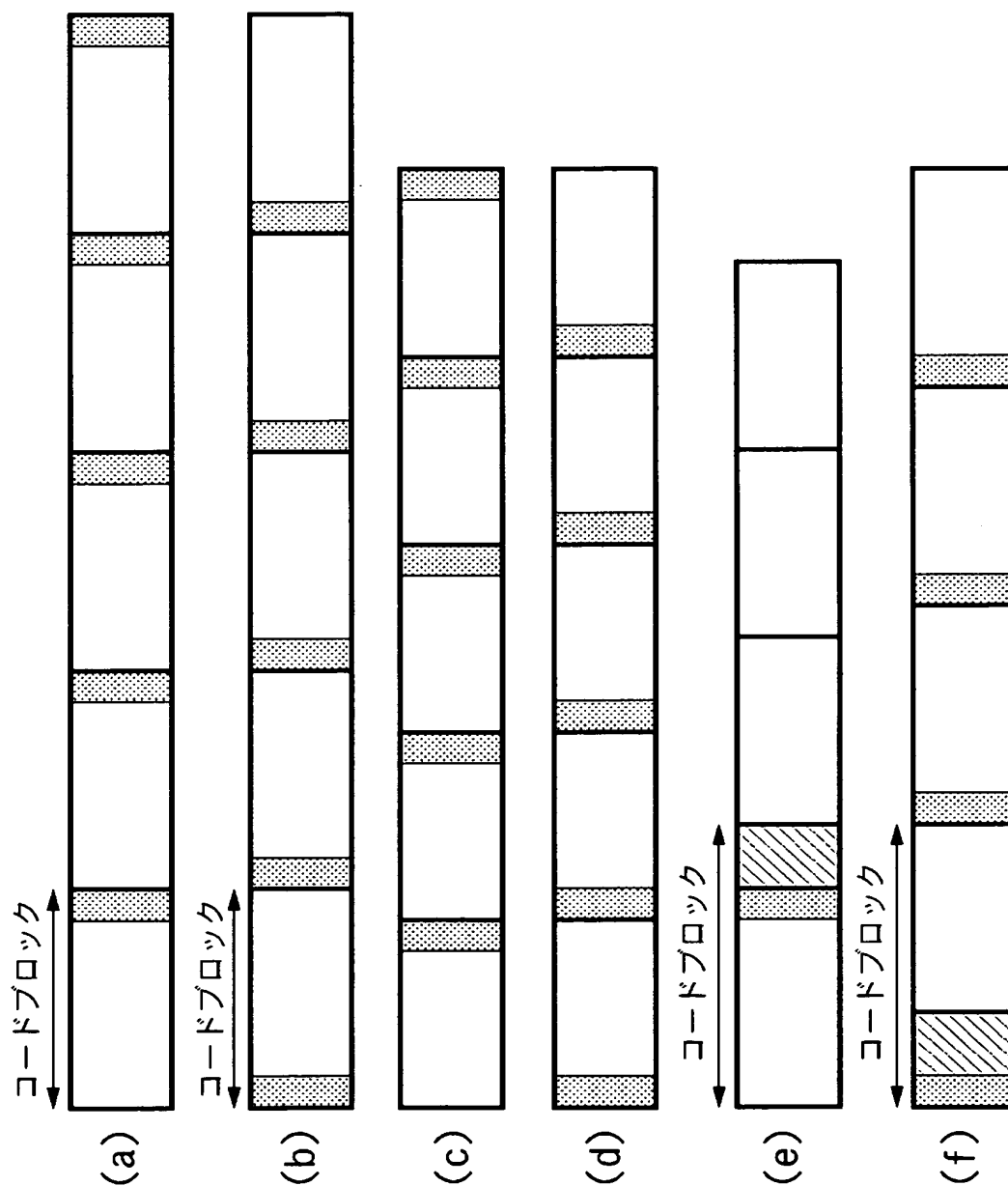
【図 4】



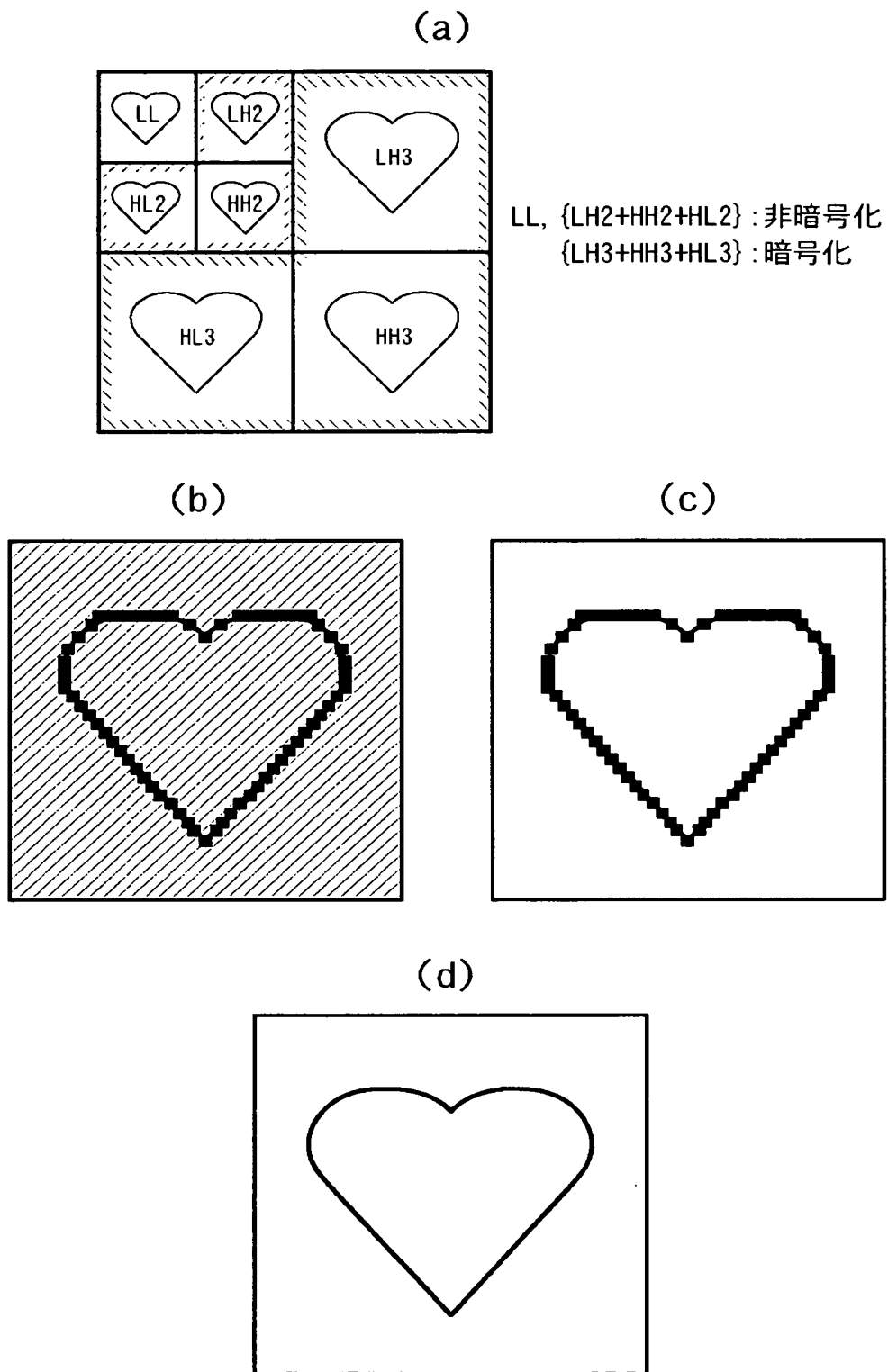
【図 5】



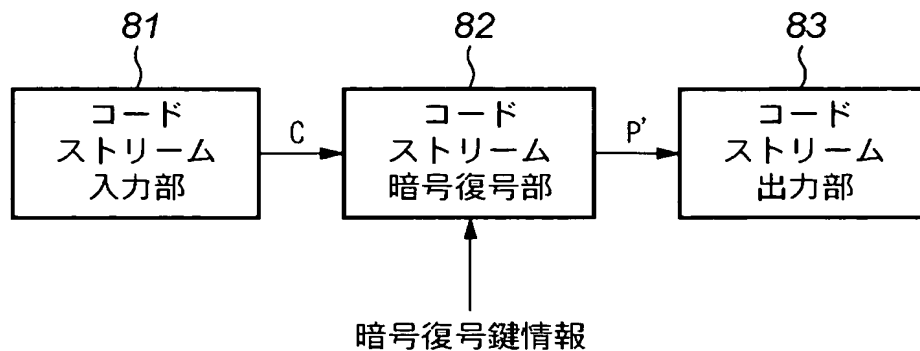
【図 6】



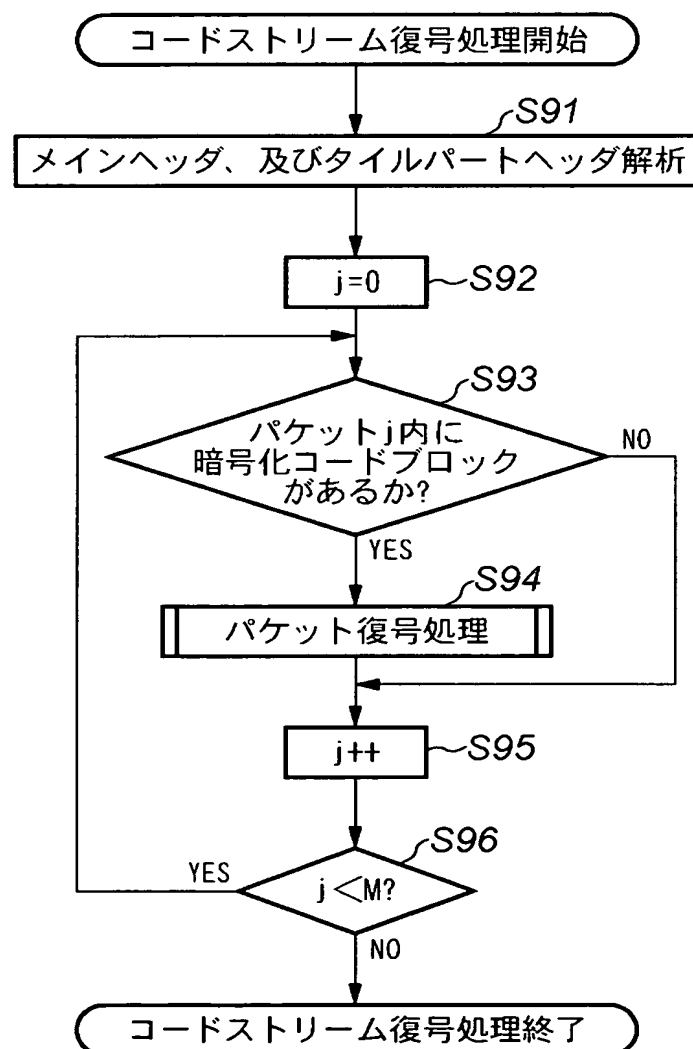
【図 7】



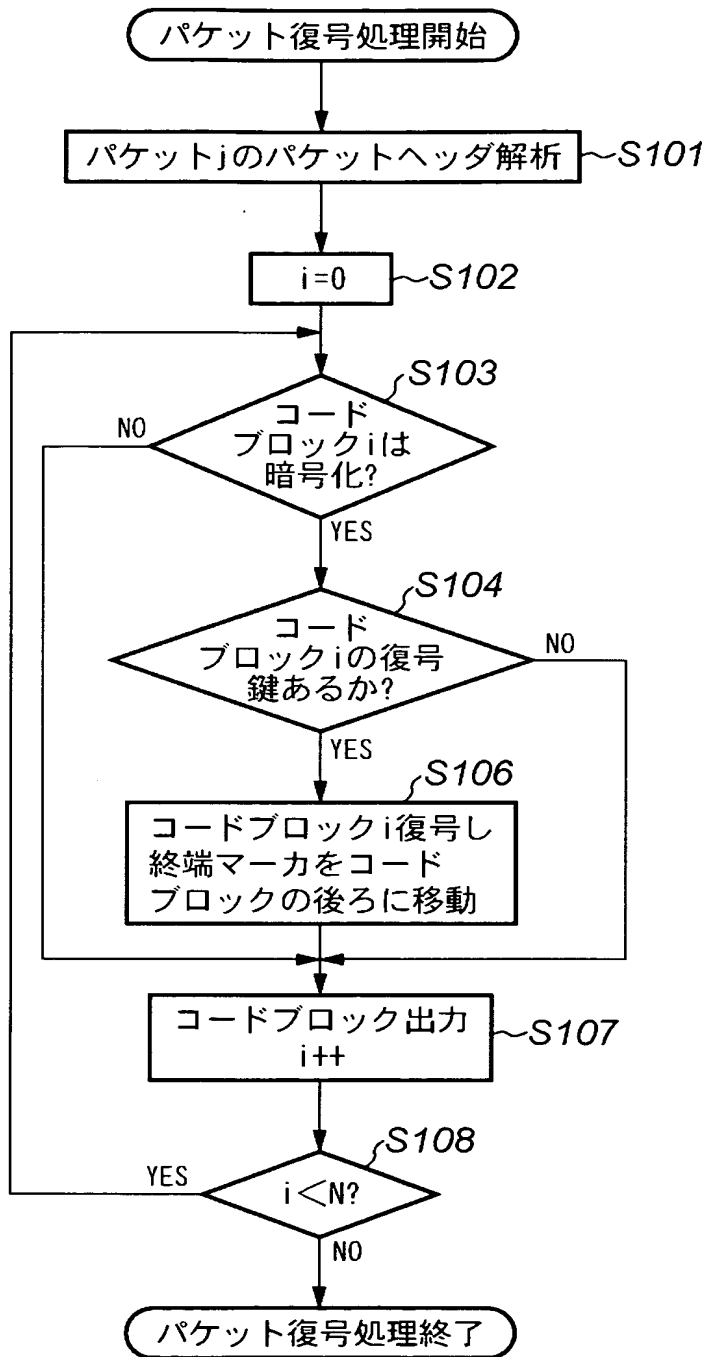
【図 8】



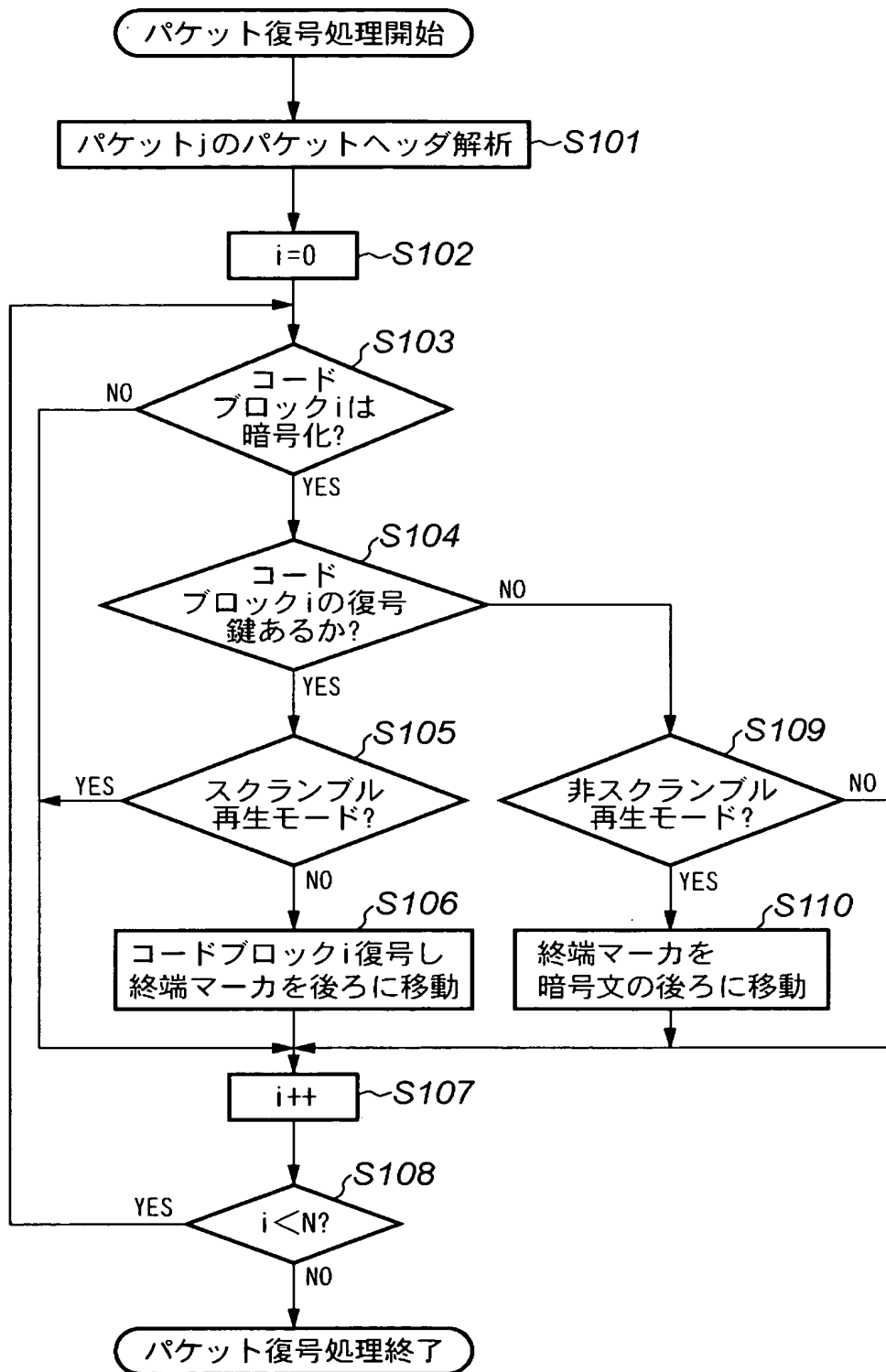
【図 9】



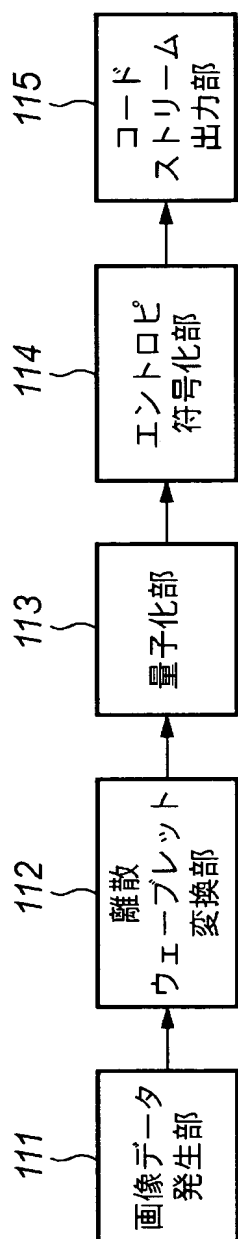
【図10A】



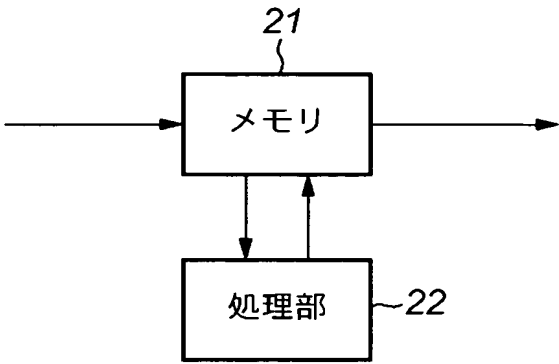
【図10B】



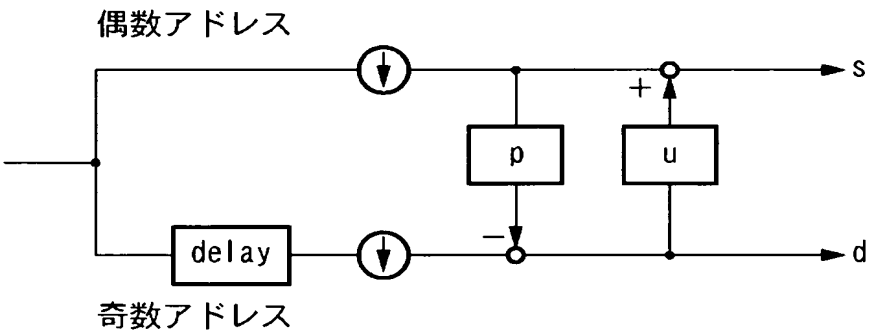
【図 11】



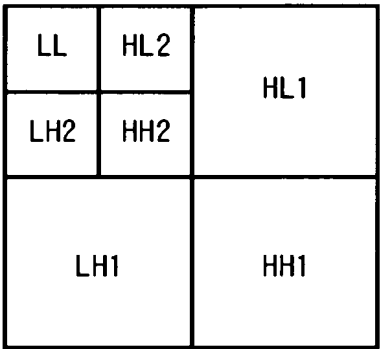
【図 1 2】



(a)

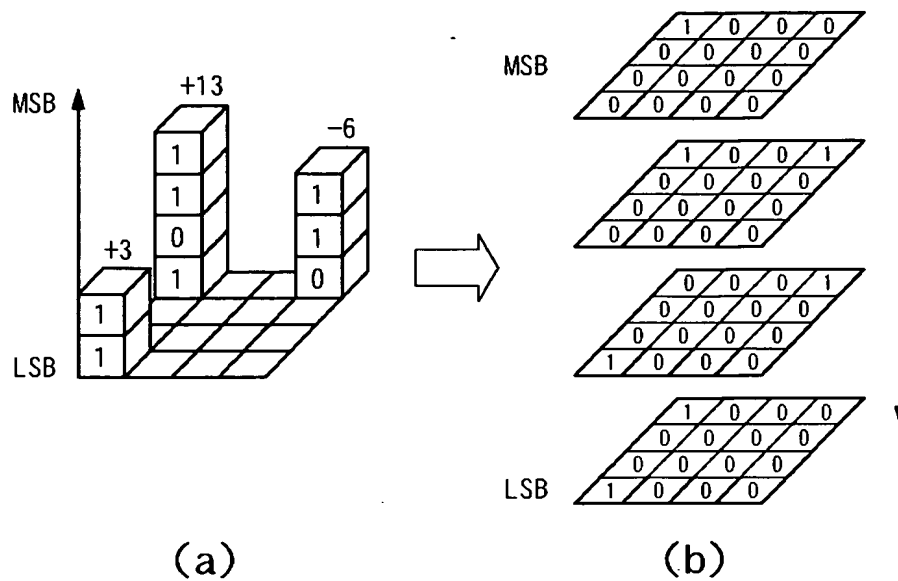


(b)

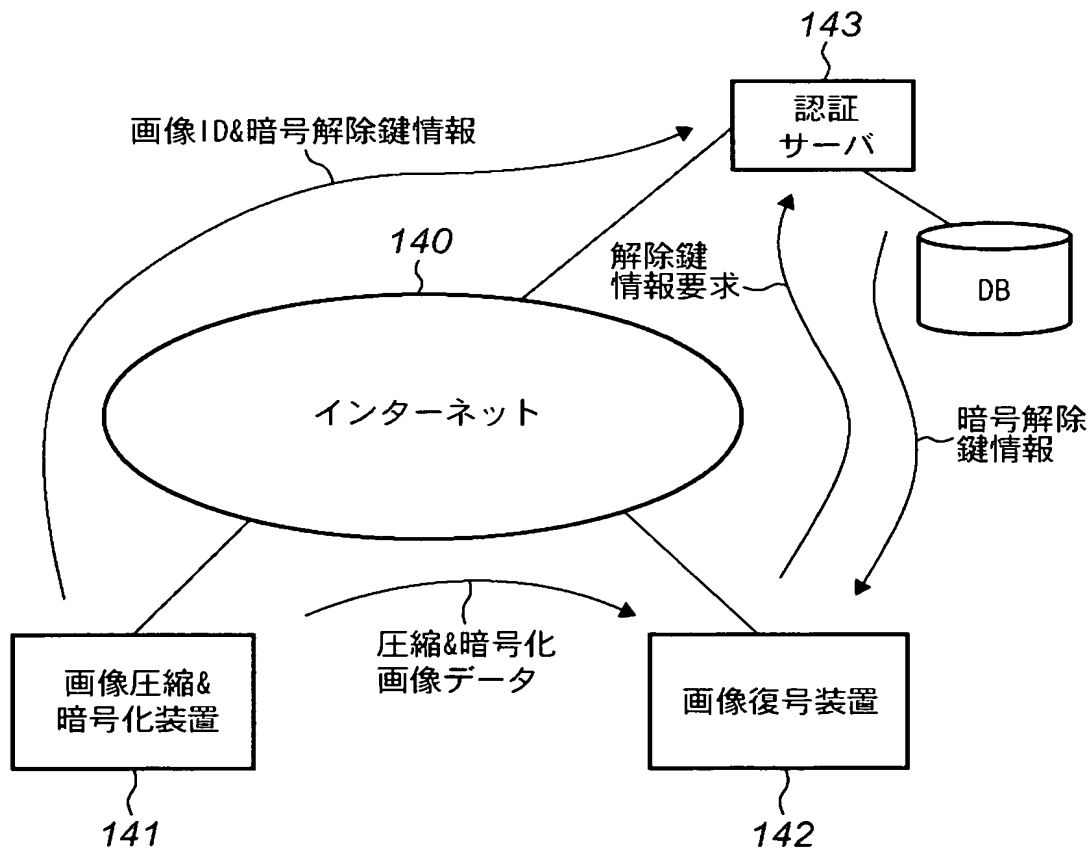


(c)

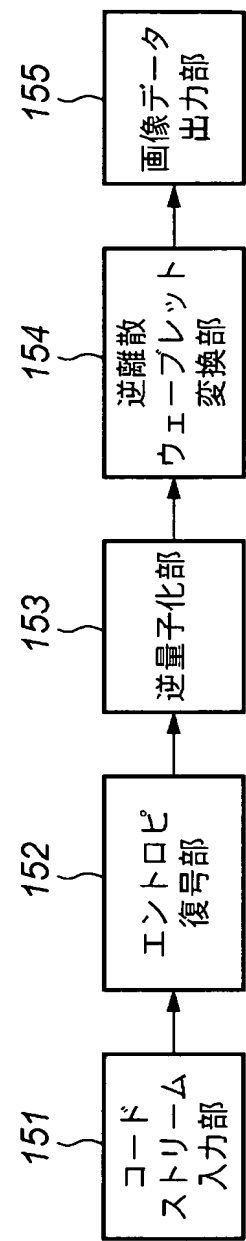
【図 13】



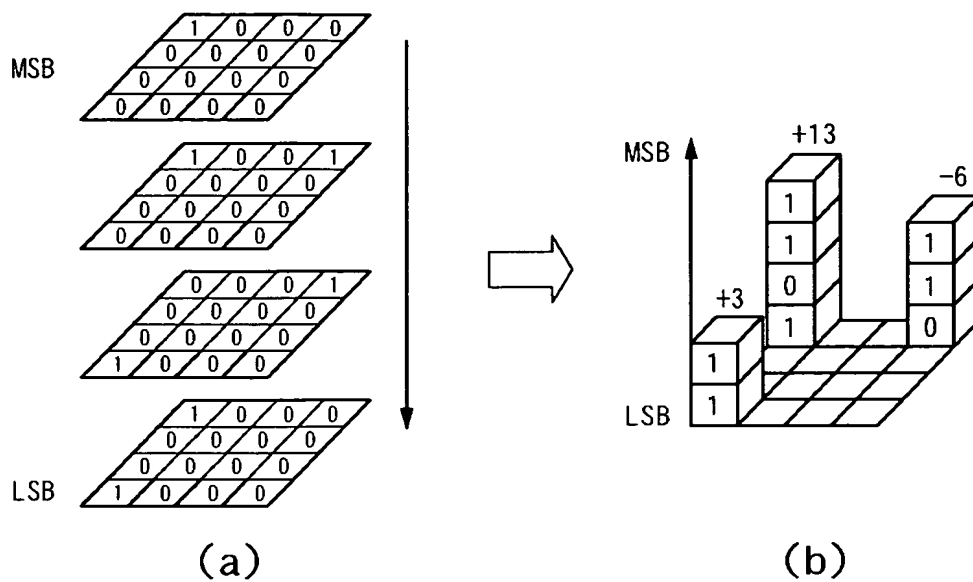
【図 14】



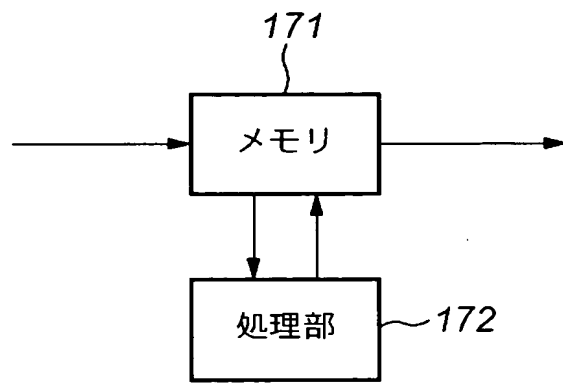
【図 15】



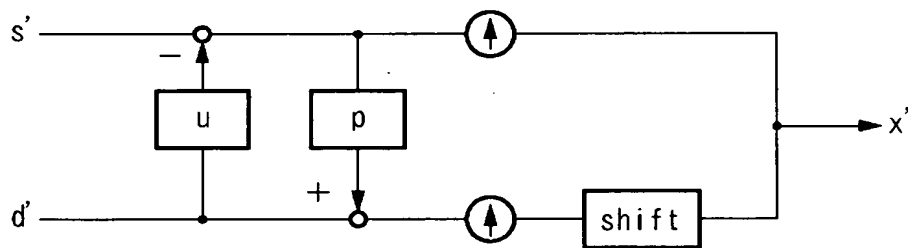
【図 16】



【図 17】

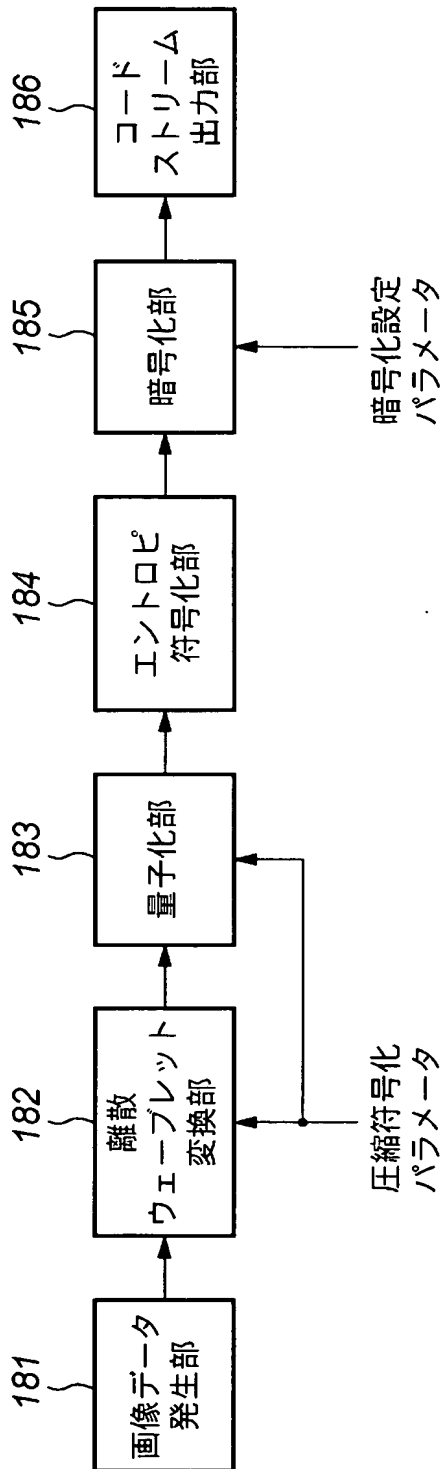


(a)

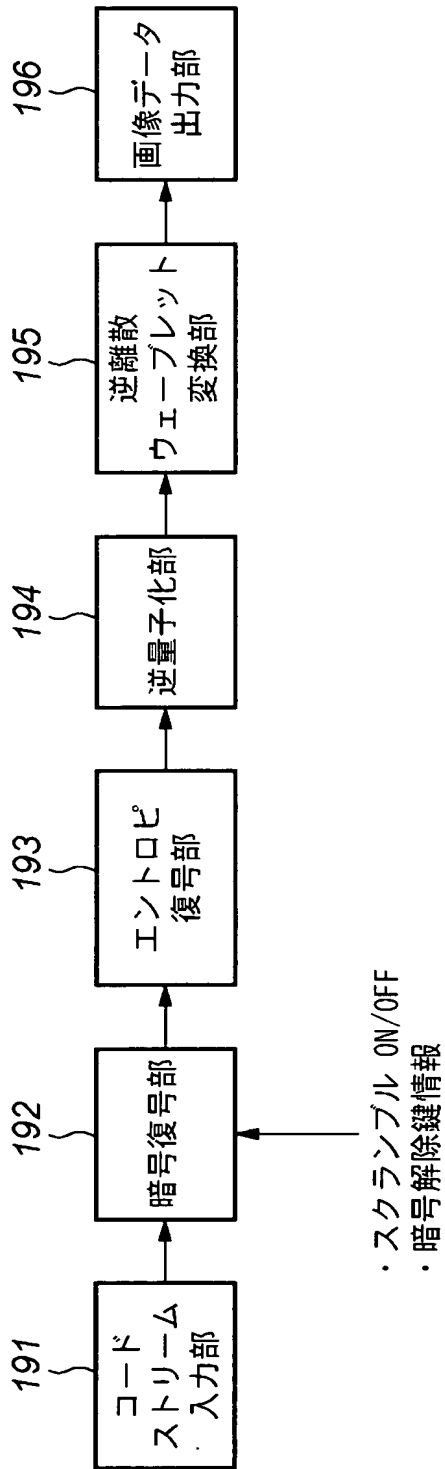


(b)

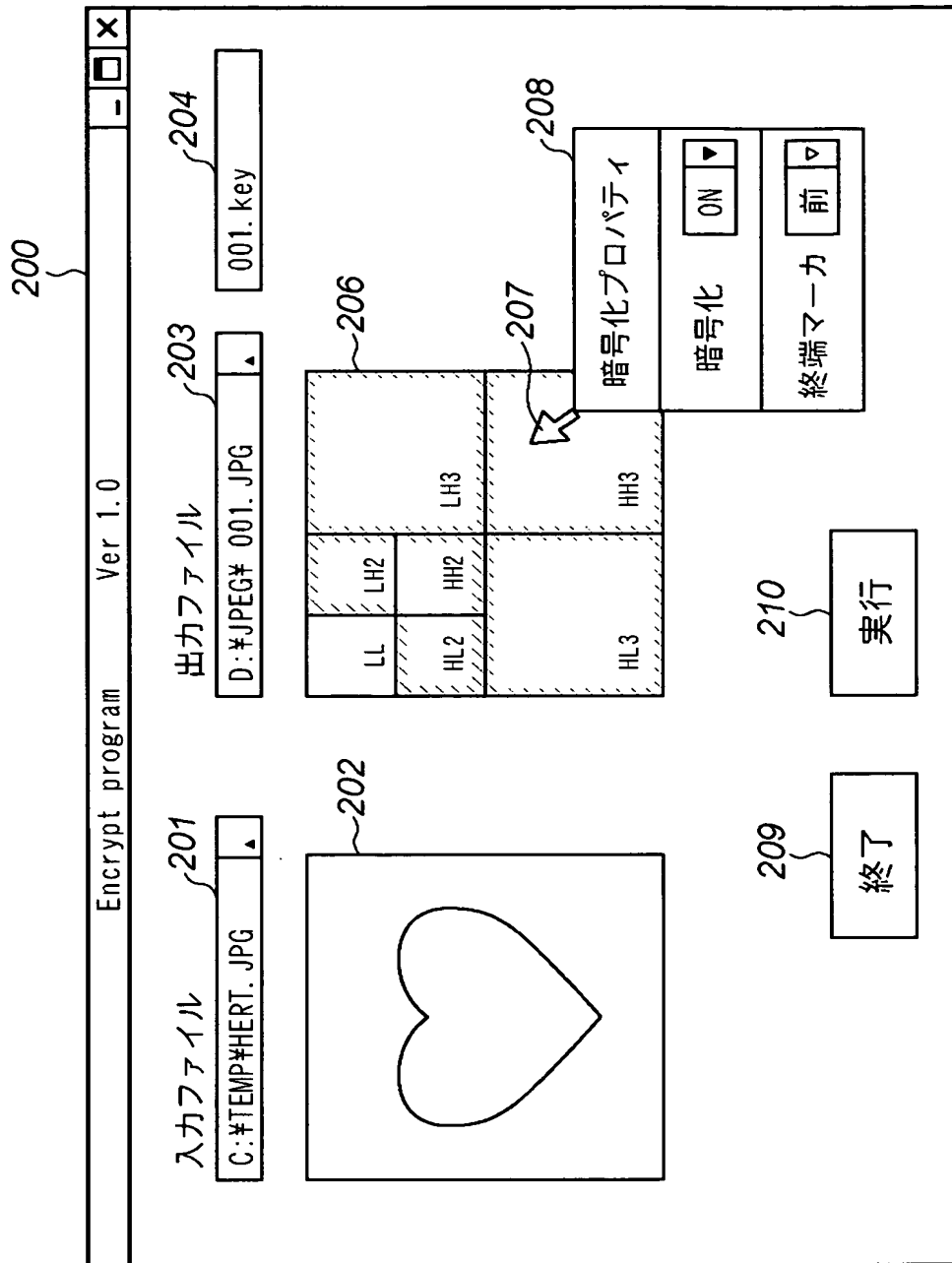
【図 18】



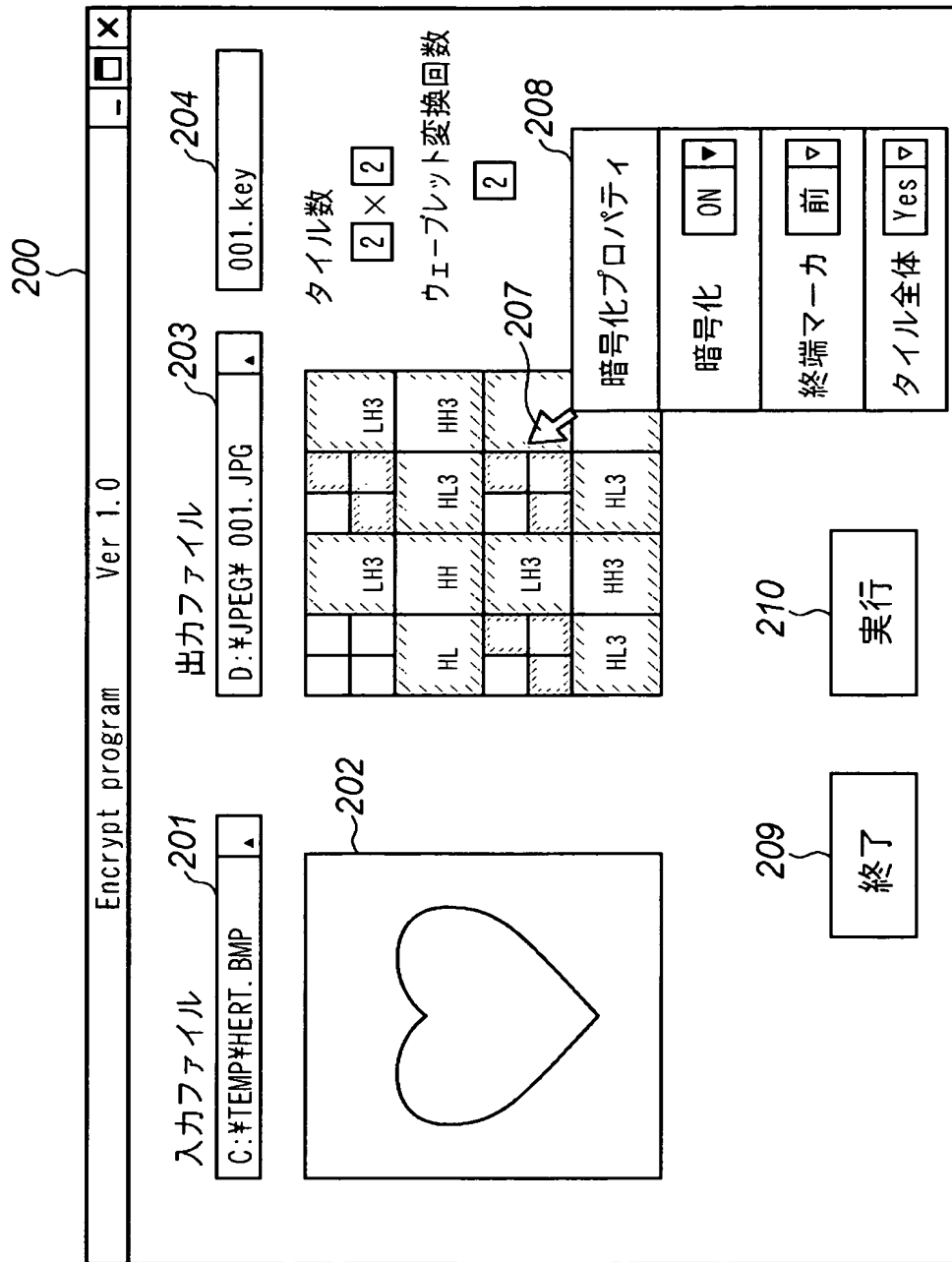
【図 19】



【図 20】



【図 21】



【書類名】 要約書

【要約】

【課題】 画像再生装置でスクランブルさせて再生させるか、或いは、非スクランブル状態で再生させるかを暗号化する側で設定可能とする。

【解決手段】 入力された画像データのコードブロックが暗号化対象であると判断した場合（S 4 3）、そのコードブロックを暗号化する（S 4 4）。そして、再生する際に、その暗号化コードブロックを利用して再生させるか（スクランブル再生モードにするか）否かを判定し（S 4 5）、その暗号化コードブロックを利用しないようにさせる場合には、終端マーカをそのコードブロックの先頭位置に配置する（S 4 7）。また、暗号化されたコードブロックを利用させる場合には終端マーカをその後端に配置する（S 4 6）。

【選択図】 図 4

特願 2 0 0 3 - 0 6 1 8 6 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 1 0 0 7]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名

キャノン株式会社